

PATENT ABSTRACTS OF JAPAN

8

(11)Publication number : 2004-318478

(43)Date of publication of application : 11.11.2004

(51)Int.Cl.

G06K 17/00
H04L 9/32

(21)Application number : 2003-111342

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 16.04.2003

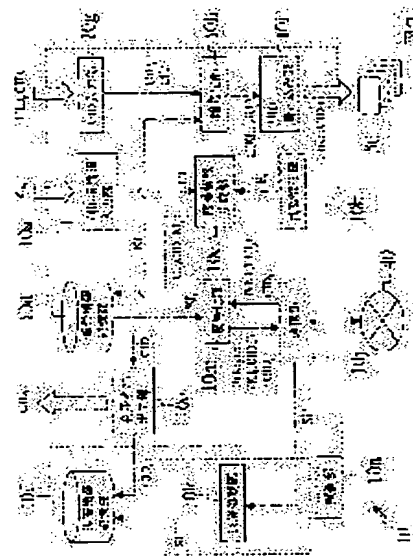
(72)Inventor : KOMURO TOMOYUKI
KINOSHITA SHINGO
HOSHINO FUMISATO
FUJIMURA AKIKO

(54) RF TAG ISSUING DEVICE, RF TAG UTILIZING DEVICE, METHOD FOR UTILIZING RF TAG, AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the forgery of an RF tag by enhancing the safety of UID stored in the RF tag.

SOLUTION: The UID inputting part 10g of an RF tag issuing device 10 accepts the input of UID to be stored in a non-contact type radio frequency tag 50. The inputted UID is converted into encrypted UID (E(Kli, UIDj)) by an encrypting part 10h. This encrypted UID (E(Kli, UIDj)) is written in the non-contact type radio frequency tag 50 by a UID writing part 10i. The radio frequency tag 50 in which the encrypted UID (E(Kli, UIDj)) is written in this way is distributed to a user. The encrypted UID (E(Kli, UIDj)) stored in the radio frequency tag 50 is decoded by an RF tag using device which the user uses.



LEGAL STATUS

[Date of request for examination]

26.03.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-318478

(P2004-318478A)

(43) 公開日 平成16年11月11日(2004.11.11)

(51) Int. Cl. 7

G06K 17/00
H04L 9/32

F I

G06K 17/00 S
G06K 17/00 F
H04L 9/00 673C
H04L 9/00 673E

テーマコード (参考)

5B058
5J104

審査請求 有 請求項の数 11 O L (全 36 頁)

(21) 出願番号 特願2003-111342 (P2003-111342)
(22) 出願日 平成15年4月16日 (2003. 4. 16)(71) 出願人 000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(74) 代理人 100066153
弁理士 草野 卓
(74) 代理人 100100642
弁理士 稲垣 稔
(72) 発明者 小室 智之
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内
(72) 発明者 木下 真吾
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

最終頁に続く

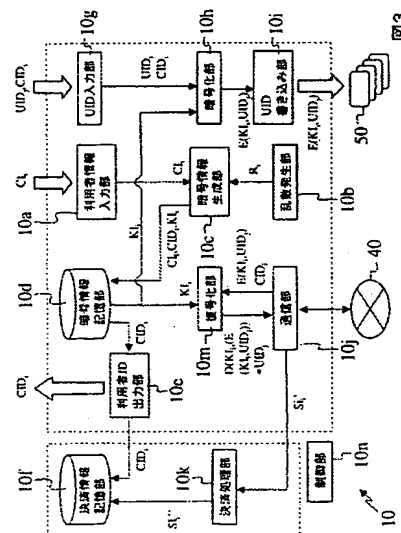
(54) 【発明の名称】 RFタグ発行装置、RFタグ利用装置、RFタグの利用方法、及びプログラム

(57) 【要約】

【課題】 RFタグに格納されたUIDの安全性を向上させ、その偽造を防止する。

【解決手段】 RFタグ発行装置10のUID入力部10gにおいて、非接触型のRFタグ50に格納するUIDの入力を受け付け、暗号化部10hにおいて、入力されたUIDを、暗号化UID ($E(KI_i, UID_i)$) に変換し、UID書き込み部10iにおいて、この暗号化UID ($E(KI_i, UID_i)$) を、非接触型のRFタグ50に書き込む。このように暗号化UID ($E(KI_i, UID_i)$) が書き込まれたRFタグ50は利用者に配布され、利用者が使用するRFタグ利用装置において、RFタグ50に格納されている暗号化UID ($E(KI_i, UID_i)$) が復号される。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

非接触型 R F タグを発行する R F タグ発行装置において、
上記非接触型 R F タグに格納する固有 I D 情報の入力を受け付ける固有 I D 情報入力手段と、

上記固有 I D 情報入力手段において入力された上記固有 I D 情報を、所定の情報を用いなければ読解が困難な情報（以下、「変換固有 I D 情報」という。）に変換する固有 I D 情報変換手段と、

上記固有 I D 情報変換手段において変換された上記変換固有 I D 情報を、上記非接触型 R F タグに書き込む変換固有 I D 情報書き込み手段と、

を有することを特徴とする R F タグ発行装置。

10

【請求項 2】

前記固有 I D 情報入力手段は、

複数の前記固有 I D 情報の入力を受け付ける手段であり、

前記固有 I D 情報変換手段は、

上記固有 I D 情報入力手段において入力された複数の上記固有 I D 情報の少なくとも一部を、入力された他の上記固有 I D 情報と異なる方法によって、前記変換固有 I D 情報に変換する手段であること、

を特徴とする請求項 1 記載の R F タグ発行装置。

20

【請求項 3】

前記変換固有 I D 情報を読解可能とするために用いる復元情報に関連付けた復元 I D 情報を、前記非接触型 R F タグに書き込む、復元 I D 情報書き込み手段を、さらに有すること

を特徴とする請求項 1 或いは 2 の何れかに記載の R F タグ発行装置。

【請求項 4】

前記変換固有 I D 情報の入力を受け付ける変換固有 I D 情報入力手段と、

上記変換固有 I D 情報入力手段において入力された上記変換固有 I D 情報を、読解可能な情報（以下、「復元固有 I D 情報」という。）に変換する固有 I D 情報復元手段と、

上記固有 I D 情報復元手段において変換された上記復元固有 I D 情報を出力する復元固有 I D 情報出力手段と、

をさらに有すること、

を特徴とする請求項 1 から 3 の何れかに記載の R F タグ発行装置。

30

【請求項 5】

前記固有 I D 情報の改ざんを防止するための改ざん防止情報を生成する改ざん防止情報生成手段と、

上記改ざん防止情報生成手段において生成された上記改ざん防止情報を前記非接触型 R F タグに書き込む、改ざん防止情報書き込み手段とを、さらに有すること、

を特徴とする請求項 1 から 4 の何れかに記載の R F タグ発行装置。

【請求項 6】

非接触型 R F タグの利用に用いる R F タグ利用装置において、

変換固有 I D 情報を読解可能とするために用いる復元情報が、復元 I D 情報に対応付けられて格納された復元情報格納手段と、

上記非接触型 R F タグから、上記復元 I D 情報を読み取る復元 I D 情報読み取り手段と、

上記復元 I D 情報読み取り手段によって読み取られた上記復元 I D 情報を用い、上記復元情報格納手段から、この復元 I D 情報に対応する上記復元情報を抽出する復元情報抽出手段と、

上記非接触型 R F タグから、上記変換固有 I D 情報を読み取る変換固有 I D 情報読み取り手段と、

上記復元情報抽出手段によって抽出された上記復元情報を用い、上記変換固有 I D 情報読み取り手段によって読み取られた上記変換固有 I D 情報を読解可能なように変換する固有

40

50

I D 情報復元手段と、
を有することを特徴とする R F タグ利用装置。

【請求項 7】

非接触型 R F タグの利用に用いる R F タグ利用装置において、
所定の情報を用いなければ読解が困難な変換固有 I D 情報を、上記非接触型 R F タグから
読み取る変換固有 I D 情報読み取り手段と、
上記変換固有 I D 情報読み取り手段によって読み取られた上記変換固有 I D 情報を出力す
る変換固有 I D 情報出力手段と、
上記変換固有 I D 情報が読解可能に変換された復元固有 I D 情報の入力を受け付ける復元
固有 I D 情報入力手段と、
を有することを特徴とする R F タグ利用装置。

10

【請求項 8】

前記非接触型 R F タグから復元 I D 情報を読み取る復元 I D 情報読み取り手段を、さらに
有し、
前記変換固有 I D 情報出力手段は、
上記復元 I D 情報読み取り手段によって読み取られた上記復元 I D 情報によって特定され
るアドレスを指定して、前記変換固有 I D 情報を出力する手段であること、
を特徴とする請求項 7 記載の R F タグ利用装置。

【請求項 9】

非接触型の R F タグの利用方法において、
R F タグ発行装置によって、
上記非接触型 R F タグに格納する固有 I D 情報の入力を受け付け、
入力された上記固有 I D 情報を、所定の情報を用いなければ読解が困難な情報（以下、「
変換固有 I D 情報」という。）に変換し、
変換された上記変換固有 I D 情報を、上記非接触型 R F タグに書き込み、
R F タグ利用装置によって、
上記非接触型 R F タグから、上記変換固有 I D 情報を読み取り、
読み取った上記変換固有 I D 情報を出力し、
上記 R F タグ発行装置によって、
上記変換固有 I D 情報の入力を受け、
入力された上記変換固有 I D 情報を、読解可能な情報（以下、「復元固有 I D 情報」とい
う。）に変換し、
上記復元固有 I D 情報を出力し、
上記 R F タグ利用装置によって、
上記復元固有 I D 情報の入力を受け付けること、
を特徴とする R F タグの利用方法。

20

30

30

【請求項 10】

請求項 1 から 5 の何れかに記載された R F タグ発行装置としてコンピュータを機能させる
ためのプログラム。

【請求項 11】

請求項 6 から 8 の何れかに記載された R F タグ利用装置としてコンピュータを機能させる
ためのプログラム。

40

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、非接触型 R F タグを発行する R F タグ発行装置、非接触型 R F タグの利用に
用いる R F タグ利用装置、この R F タグの利用方法、及びそれらの機能をコンピュータに
実行させるためのプログラムに関し、特に、取り扱う情報の安全性の向上を図った R F タ
グ発行装置、R F タグ利用装置、R F タグの利用方法、及びプログラムに関する。

【0002】

50

【従来の技術】

近年、RFID (Radio Frequency Identification: 電波方式認識) の導入が様々な分野で進んでいる (例えば、非参照文献1参照。)。RFIDは、「RFタグ」と呼ばれる小型の情報記録媒体と、「リーダー」と呼ばれる質問器との間で非接触の情報交信を行う技術であり、人の出入りが激しい店舗での万引き防止等のセキュリティ目的の他、商品を取り出さずに検品ができるという利点から、倉庫・運送等の物流管理においても特に有用な技術である。

このRFIDに使用されるRFタグは、非接触ICチップを用いた記録媒体及びアンテナが埋め込まれたプレート (タグ) であり、この記録媒体には「UID: Unique Identify」と呼ばれる各用途に応じた固有値が書き込まれている。通常、このRFタグは、衣類や電荷製品等の商品に取り付けられて使用され、このRFタグが取り付けられた商品の商品識別番号・商品固体番号等の情報は、そのRFタグに格納されたUIDに関連付けて外部のデータベースに保管される。そして、店員等の利用者は、リーダーを用いてRFタグからUIDを読み取り、読み取ったUIDをこのデータベースの情報と照合することにより、そのRFタグが取り付けられている商品の商品識別番号・商品固体番号等を知ることができる。

【0003】

【非特許文献1】

Auto-ID Center, "About the technology", [online], [平成15年4月9日検索]、インターネット<<http://www.auto-id-center.org/about-the-center.asp>>

【0004】

【発明が解決しようとする課題】

しかし、従来のRFタグでは、格納されたUIDの安全性が十分ではないという問題点がある。

つまり、RFタグは、商品とともに流通過程を転々とし、商品が消費者の手に渡った後もその商品と一体に存在する場合がある。そして、このRFタグに格納されたUIDは、それを読み取るリーダーを有し、このUIDにアクセスするプロトコルを知っているものであれば、誰でもその内容を読み取ることができる。従って、例えば、甲が乙の所持しているRFタグ付の商品を遠隔から読み取り、読み取ったUIDと商品との対応を調べることで、この甲は乙の所持品を容易に知ることができる。そして、このRFタグ付の商品がプライベートなものであればあるほど、乙のプライバシーが侵害される可能性が高くなる。

【0005】

また、従来のRFタグでは、それに格納されているUIDを容易に偽造できてしまうという問題点もある。

つまり、RFタグ付の商品の入手者は、上述のように、RFタグに格納されたUIDを容易に読み取ることができ、この読み取ったUIDと商品との対応を調べることで、特定の商品のUIDを容易に推測できてしまう。これは、UIDの設定は、UIDを使用する際の利便性やコストを考慮し、何らかのルールに従って行われることが通常だからである。そのため、例えば、ブランドや流通過程等を偽った商品に、この偽造したUIDを格納したRFタグを付すことにより、UIDの内容までも再現した偽造商品を容易に製造できてしまう。

【0006】

また、このような点に考慮し、パスワード等の秘密情報を安全に保管する耐タンパー性を備えた記録媒体と、この秘密情報による認証処理等のアクセス制御を行うICチップとをRFタグ内に実装したものもあるが、このようなRFタグの価格は高く、個々の商品にこのようなRFタグを付与することはコストの面から現実的ではない。

この発明はこのような点に鑑みてなされたものであり、格納するUIDの安全性を向上させ、その偽造を防止できる安価なRFタグを発行するRFタグ発行装置を提供することで

ある。

【 0 0 0 7 】

また、この発明の他の目的は、格納された U I D の安全性を向上させ、その偽造を防止できる安価な R F タグの利用に用いる R F タグ利用装置を提供することである。

さらに、この発明の他の目的は、低コストで、R F タグに格納された U I D の安全性を向上させ、その偽造の防止を可能にする R F タグの利用方法を提供することである。

また、この発明の他の目的は、低コストで、R F タグに格納された U I D の安全性を向上させ、その偽造の防止を可能にする機能をコンピュータに実行させるためのプログラムを提供することである。

【 0 0 0 8 】

10

【課題を解決するための手段】

この発明では上記課題を解決するために、まず、非接触型 R F タグに格納する固有 I D 情報 (U I D) の入力を受け付け、入力された固有 I D 情報を、所定の情報を用いなければ読解が困難な情報 (変換固有 I D 情報) に変換する。そして、この変換された変換固有 I D 情報を、非接触型の R F タグに書き込む。

ここで、このように発行された R F タグの内容を悪意の者が読み取ったとしても、この者が知り得る情報は変換固有 I D 情報のみであり、固有 I D 情報自体の内容を知ることにはできない。これにより、R F タグに格納された U I D の安全性向上と、その偽造の防止を図ることができる。さらに、R F タグに秘密情報を保持するための構造や、認証処理を行うための I C を必要としないため、R F タグのコストも安い。

20

【 0 0 0 9 】

また、この発明において、好ましくは、I D 情報の改ざんを防止するための改ざん防止情報を、非接触型 R F タグに書き込む。これにより、R F タグの内容が偽造されたとしても、この改ざん防止情報を検証することにより、容易にその偽造を発見することができる。

【 0 0 1 0 】

【発明の実施の形態】

以下、この発明の実施の形態を図面を参照して説明する。

〔第 1 の実施の形態〕

この形態は、R F タグ発行装置において、U I D (U n i q u e I D e n t i f y) を共通鍵によって暗号化して R F タグに書き込み、R F タグ利用装置からこの R F タグ発行装置に対し、暗号化された U I D の復号を依頼する形態である。なお、この形態で使用する暗号化アルゴリズムは、共通鍵暗号方式であれば、D E S 等特に制限はなく、R F タグ発行装置、R F タグ利用装置間において、予め取決め・設定しておくものとする。

【 0 0 1 1 】

図 1 は、この形態における R F タグ利用システム 1 の全体を例示した概念図である。

図 1 に例示するように、この例の R F タグ利用システム 1 は、非接触型の R F タグ 5 0 を発行する R F タグ発行装置 1 0、この R F タグ 5 1 ~ 5 3 の利用に用いる複数の R F タグ利用装置 2 1 ~ 2 3、及び決済処理を行う決済処理サーバ装置 3 0 によって構成され、これらは物理的又は理論的に安全なネットワーク 4 0 によって、相互に通信可能なように構成されている。なお、この R F タグ発行装置 1 0 は、例えば、セキュリティサービスを行う会社が運営し、R F タグ利用装置 2 1 ~ 2 3 は、R F タグを使用する店舗等に配置されるものである。

【 0 0 1 2 】

図 2 の (a) は、図 1 に例示した R F タグ発行装置 1 0 のハードウェア構成を例示したブロック図であり、図 2 の (b) は、R F タグ利用装置 2 1 のハードウェア構成を例示したブロック図である。

図 2 の (a) に例示するように、この例の R F タグ発行装置 1 0 は、C P U (C e n t r a l P r o c e s s i n g U n i t) 1 1、キーボード等の入力装置 1 2、液晶ディスプレイ等の出力装置 1 3、ハードディスク等の外部記憶装置 1 4、電磁気的な方法により非接触で R F タグに情報を書き込む書き込み装置 1 5、R A M (R a n d o m A c c

50

ess Memory)、ROM (Read Only Memory)等の半導体記憶装置16、ネットワーク40と通信可能なように接続され、このネットワーク40を介した通信を可能にする通信制御装置17、及びこれらを情報のやり取りが可能なように接続するバス18を有している。

【0013】

また、図2の(b)に例示するように、この例のRFタグ利用装置21は、CPU20a、入力装置20b、出力装置20c、外部記憶装置20d、電磁気的な方法により非接触でRFタグから情報を読み取る読み取り装置20e、半導体記憶装置20f、ネットワーク40と通信可能なように接続され、このネットワーク40を介した通信を可能にする通信制御装置20g、及びこれらを情報のやり取りが可能なように接続するバス20hを有している。 10

なお、その他のRFタグ利用装置22、23のハードウェア構成も、RFタグ利用装置21と同様であり、また、決済処理サーバ装置30のハードウェア構成は、RFタグ発行装置10から書き込み装置15を除いたものと同様である。

【0014】

図3は、図2の(a)に例示したハードウェア構成において所定のプログラムを実行させることによって構成されるRFタグ発行装置10の機能構成の例示であり、図4は、このRFタグ発行装置10の暗号情報記憶部10dに格納される暗号データベース1001のデータ構成を例示した図であり、図5は、RFタグ50に格納されるデータの構成を例示した概念図である。また、図6は、図2の(b)に例示したハードウェア構成において所定のプログラムを実行させることによって構成されるRFタグ利用装置21の機能構成の例示であり、図7は、このRFタグ利用装置21に格納されるUIDデータベース1003の構成を例示した概念図である。また、図8の(a)及び(c)は、この例のRFタグ発行装置10の処理を説明するためのフローチャートであり、(b)は、この例のRFタグ利用装置21の処理を説明するためのフローチャートである。 20

【0015】

以下、これらの図を用いて、本形態におけるRFタグ発行装置10及びRFタグ利用装置21の機能構成及び処理について説明を行っていく。なお、RFタグ発行装置10の制御は制御部10hによって、RFタグ利用装置21の制御は制御部21gによって行われる。また、他のRFタグ利用装置22、23の機能構成及び処理は、以下のRFタグ利用装置21のものと同様である。 30

また、以下においてE、Dは、それぞれ暗号化関数、復号関数を意味し、E(a, b)は、鍵aにより暗号化関数Eを用いてbを暗号化する処理を意味し、D(a, b)は、鍵aにより復号関数Dを用いてbを復号する処理を意味する。

【0016】

RFタグの発行：

まず、RFタグ発行の前提として、RFタグの利用者(商品販売業者、サービス提供者等)の登録を行うため、RFタグ発行装置10の利用者情報入力部10aから利用者情報(CI_i)の入力を受け付ける(ステップS1)。入力された利用者情報(CI_i)は暗号情報生成部10cに送られ、暗号情報生成部10cは、これに対応する利用者ID(CID_i)を生成する。また、乱数発生部10bにおいて、SHA-1等の一方向性ハッシュ関数を用いて構成される疑似乱数生成アルゴリズム等を用いて(疑似)乱数(R_i)を発生させ、この乱数(R_i)を暗号情報生成部10cに送る。暗号情報生成部10cでは、これらの情報を用い、共通鍵情報(KI_i)を生成し、生成した共通鍵情報(KI_i)と利用者ID(CID_i)を、利用者情報(CI_i)とともに暗号情報記憶部10dに送り、そこで暗号データベース1001として記憶させる(ステップS2)。 40

【0017】

図4の例の場合、この暗号データベース1001は、利用者ID(CID_i)1001a、利用者情報(CI_i)1001b及び共通鍵情報(KI_i)が相互に関連付けられることによって構成され、利用者ID(CID_i)「AA111111」「AA111112」 50

「A A 1 1 1 1 1 3」「A A 1 1 1 1 1 4」に対し、共通鍵情報 ($K I_i$) 「1 2 3 4」「1 3 5 7」「2 4 6 8」「9 8 7 6」がそれぞれ対応している。なお、このように記録された利用者ID ($C I D_i$) は、利用者ID出力部10eから出力され、郵送等によって各利用者に安全に通知される。

次に、UID入力部10gにおいて、商品ID等の所定の情報に関連付けられたUID_j及びRFタグを発行する利用者の利用者ID ($C I D_i$) の入力を受け付け、それらを暗号化部10hに送る(ステップS4)。暗号化部10hでは、受け取った利用者ID ($C I D_i$) に対応する共通鍵情報 ($K I_i$) を、暗号情報記憶部10dの暗号データベース1001から抽出し、この共通鍵情報 ($K I_i$) を用い、UID_jを暗号化 ($E (K I_i, U I D_j)$) する(ステップS5)。

10

【0018】

この暗号化されたUID_jである暗号化UID ($E (K I_i, U I D_j)$) は、UID書き込み部10iに送られ、そこで、RFタグ50の暗号化UID領域50a(図5)に書き込まれる(ステップS6)。なお、RFタグ50のユーザ領域50bは、後の流通過程等において利用者が自由に情報(価格情報、温度管理情報、産地等)を読み書きできる領域である。

RFタグの利用:

上述のように暗号化UIDが書き込まれたRFタグ51~53は、各利用者に配布され、利用者はこのRFタグ51~53を商品等に取り付ける。取り付けられたRFタグ51~53は、例えば、商品の在庫管理等の際に、RFタグ利用装置21~23によって読み取られる。以下、RFタグ51の利用手順を例にとって説明を行う。

【0019】

RFタグ51を利用する店舗等では、まず、このRFタグ51に格納された暗号化UIDの復号を依頼のための決済入力(クレジットカード番号等)を行う。この決済入力 ($S I_i$) は、RFタグ利用装置21の決済処理情報入力部21cにおいて受け付けられ(ステップS10)、通信部21dに送られ、そこからネットワーク40を介し、決済処理を行う決済処理サーバ装置30に送られる(ステップS11)。

次に、利用者ID入力部21bにおいて利用者ID ($C I D_i$) の入力を受け付け(ステップS12)、さらに、RFタグ読み取り部21aにおいてRFタグ51の暗号化UID ($E (K I_i, U I D_j)$) を読み取る(ステップS13)。これらの利用者ID ($C I D_i$) 及び暗号化UID ($E (K I_i, U I D_j)$) は、それぞれ通信部21dからネットワーク40を介してRFタグ発行装置10に送信される(ステップS14)。送信されたこれらの情報 ($C I D_i, E (K I_i, U I D_j)$) は、RFタグ発行装置10の通信部10jにおいて受信され(ステップS20)、復号化部10mに送られる。

【0020】

復号化部10mでは、受け取った利用者ID ($C I D_i$) に対応する共通鍵情報 ($K I_i$) を暗号情報記憶部10dの暗号データベース1001から抽出し、この共通鍵情報 ($K I_i$) を用いて、暗号化UID ($E (K I_i, U I D_j)$) を復号 ($D (K I_i, E (K I_i, U I D_j)) = U I D_j$) する(ステップS21)。

その後、通信部10j、ネットワーク40を介して決済処理サーバ装置30にアクセスし、そこで決済処理を行った後、この決済処理サーバ装置30から出力される決済出力情報 ($S i_i'$) をネットワーク40を介して通信部10jで受信する。この決済出力情報 ($S i_i'$) は、さらに決済処理部10kで処理され、その出力情報 ($S i_i''$) は決済情報記憶部10fに送られて記憶される(ステップS22)。この際、この出力情報 ($S i_i''$) は、例えば、利用者ID出力部10eから送られた利用者ID ($C I D_i$) に対応付けて記憶される。

【0021】

次に、復号化部10mは、復号したUID_jを通信部10jに送り、そこからネットワーク40を介し、RFタグ利用装置21に、このUID_jを送信する(ステップS23)。送信されたUID_jは、通信部21dによって受信され(ステップS15)、タグ情報抽

50

出部 21e に送られる。ここで、UID データ記憶部 21f には、UID (UID_j) 1003a と商品 ID (PID_k) を対応付けた UID データベース 1003 が格納されており (この例では、UID_j=123, 456, 789, 101, 102 に対して、PID_k=LV0001, LV0002, GR000, GR0002 が対応付けられている (図 7)。)、タグ情報抽出部 21e は、送られた UID_j に対応する商品 ID (PID_k) を UID データ記憶部 21f から抽出し、出力する (ステップ S16)。

【0022】

このように、この形態の RF タグ発行装置 10 では、固有 ID 情報入力手段である UID 入力部 10g において、非接触型の RF タグ 50 に格納する固有 ID 情報 (UID) の入力を受け付け、固有 ID 情報変換手段である暗号化部 10h において、入力された固有 ID 10 D 情報を、所定の情報を用いなければ読解が困難な情報 (変換固有 ID 情報) である暗号化 UID (E (K_I, UID_j)) に変換し、変換固有 ID 情報書き込み手段である UID 書き込み部 10i において、この暗号化 UID (E (K_I, UID_j)) を、非接触型の RF タグ 50 に書き込むこととした。

そのため、このように発行された RF タグ 50 の内容を悪意の者が読み取ったとしても、この者が知り得る情報は暗号化 UID (E (K_I, UID_j)) のみであり、この者は UID 自体の内容を知ることができない。その結果、RF タグ 50 の UID の内容が第三者に読み取られ、商品所有者のプライバシーが侵害されることもない。

【0023】

また、第三者は、RF タグ 50 に格納された UID の内容を読み取ることができないため 20、この UID と商品の対応から特定の商品の UID を推測することも容易ではない。その結果、UID の偽造をも防止することができる。

さらに、暗号化 UID (E (K_I, UID_j)) 自体は秘密情報でないため、RF タグ 50 に秘密情報を保持するための構造や、認証処理を行うための IC を必要とせず、RF タグ 50 のコストも安い。

また、この形態の RF タグ発行装置 10 では、変換固有 ID 情報入力手段である通信部 10j において、変換固有 ID 情報である暗号化 UID (E (K_I, UID_j)) の入力を受け付け、固有 ID 情報復元手段である復号化部 10m において、この暗号化 UID (E (K_I, UID_j)) を、読解可能な情報 (復元固有 ID 情報) である UID_j に復号 (変換) し、復元固有 ID 情報出力手段である通信部 10j において、安全なネットワ 30ーク 40 を介して、この UID_j を出力することとした。

【0024】

さらに、この形態の RF タグ利用装置 21 では、変換固有 ID 情報読み取り手段である RF タグ読み取り部 21a において、所定の情報を用いなければ読解が困難な情報 (変換固有 ID 情報) である暗号化 UID (E (K_I, UID_j)) を非接触型 RF タグ 51 から読み取り、変換固有 ID 情報出力手段である通信部 21d において、この暗号化 UID (E (K_I, UID_j)) を RF タグ発行装置 10 に出力し、復元固有 ID 情報入力手段である通信部 21d において、RF タグ発行装置 10 から返送された復元固有 ID 情報 (変換固有 ID 情報が読解可能に変換された情報) である UID_j の入力を受け付けることとした。 40

【0025】

これにより、暗号化 UID を復号するための鍵情報 (K_I) を RF タグ発行装置 110 のみで安全に管理することが可能となり、悪意の第三者に暗号化 UID (E (K_I, UID_j)) が復号され、商品所有者のプライバシー侵害や UID の偽造等が生じるといった事態を効果的に阻止することできる。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態では、利用者 ID (CID_i) を利用者ごとに設定することとしたが、所定の業種ごと、所定の商品ごと、所定の製造日ごとに、この利用者 ID (CID_i) を設定することとしてもよい。

【0026】

〔第 2 の実施の形態〕

この形態は、公開鍵暗号方式によって U I D を暗号化し、R F タグに格納する形態である。なお、第 1 の実施の形態と共通する事項については説明を省略する（以下の他の形態についても同様。）。なお、この形態で使用する暗号化アルゴリズムは、公開鍵暗号方式であれば、R S A 等特に制限はなく、R F タグ発行装置、R F タグ利用装置間において、予め取決め・設定しておくものとする。

図 9 は、この形態における R F タグ利用システム 1 0 1 の全体を例示した概念図である。

〔 0 0 2 7 〕

図 9 に例示するように、この例の R F タグ利用システム 1 0 1 は、R F タグ 1 5 0 を発行する R F タグ発行装置 1 1 0、R F タグ 1 5 1 ~ 1 5 3 の利用に用いる R F タグ利用装置 1 2 1 ~ 1 2 3、及び公開鍵証明書を発行する認証局装置 1 3 0 によって構成され、これらは物理的又は理論的に安全なネットワーク 1 4 0 によって、相互に通信可能なように構成されている。

図 1 0 は、図 2 の (a) と同様なハードウェア構成において所定のプログラムを実行させることによって構成される R F タグ発行装置 1 1 0 の機能構成の例示であり、図 1 1 は、R F タグ 1 5 0 のデータ構成の例示であり、図 1 2 は、図 2 の (b) と同様なハードウェア構成において所定のプログラムを実行させることによって構成される R F タグ利用装置 1 2 1 の機能構成の例示である。また、図 1 3 の (a) は、R F タグ発行装置 1 1 0 の処理を説明するためのフローチャートであり、(b) は、R F タグ利用装置 1 2 1 の処理を説明するためのフローチャートである。

20

〔 0 0 2 8 〕

以下、これらの図を用いて、本形態における R F タグ発行装置 1 1 0 及び R F タグ利用装置 1 2 1 の機能構成及び処理について説明を行っていく。なお、R F タグ発行装置 1 1 0 の制御は制御部 1 1 5 によって、R F タグ利用装置 1 2 1 の制御は制御部 1 2 1 g によって行われる。また、他の R F タグ利用装置 1 2 2、1 2 3 の機能構成及び処理は、以下の R F タグ利用装置 1 2 1 のものと同様である。

R F タグの発行：

まず、R F タグ利用装置 1 2 1 の U I D 入力部 1 2 1 a において、U I D_jの入力を受け付け、入力された U I D_jを通信部 1 2 1 c に送る。また、ネットワーク 1 4 0 を介して認証局装置 1 3 0 から取得し、鍵情報記憶部 1 2 1 b に記憶されている公開鍵証明書 (C e r t P K_e (P K_i)) を読み出し、通信部 1 2 1 c に送る。これらの情報が送られた通信部 1 2 1 c は、これらの U I D_j及び公開鍵証明書 (C e r t P K_e (P K_i)) を、ネットワーク 1 4 0 を介し、R F タグ発行装置 1 1 0 に送る。なお、S K_eは認証局装置 1 3 0 の秘密鍵を、P K_iは R F タグ利用装置 1 2 1 の公開鍵を意味する。

30

〔 0 0 2 9 〕

これらの情報が送られた R F タグ発行装置 1 1 0 は、通信部 1 1 1 によって、これら (U I D_j, C e r t P K_e (P K_i)) を受信する。また、通信部 1 1 1 は、ネットワーク 1 4 0 を介し、認証局装置 1 3 0 から認証局装置 1 3 0 の公開鍵 P K_eを取得する (ステップ S 3 0) 。

通信部 1 1 1 に受信された公開鍵証明書 (C e r t P K_e (P K_i)) 及び認証局装置 1 3 0 の公開鍵 P K_eは、公開鍵検証部 1 1 2 に送られ、この公開鍵検証部 1 1 2 は、(V e r i f y P K_e (C e r t P K_e (P K_i))) = O K o r N G を検証する (ステップ S 3 1) 。ここで、N G となれば、公開鍵 P K_eを拒否する旨の信号を暗号化部 1 1 3 に送って処理を終了し (ステップ S 3 2) 、O K となれば、公開鍵 P K_eを受諾する旨の信号を暗号化部 1 1 3 に送り、暗号化部 1 1 3 は、通信部 1 1 1 から U I D_jと公開鍵 P K_iを取得し、この公開鍵 P K_iで U I D_jを暗号化 (E (P K_i, U I D_j)) する (ステップ S 3 3) 。

40

〔 0 0 3 0 〕

このように暗号化された E (P K_i, U I D_j) (暗号化 U I D) は、U I D 書き込み部 1 1 4 に送られ、そこで R F タグ 1 5 0 の暗号化 U D I 領域 1 5 0 a に書き込まれる (ス 50

テップ S 3 4)。そして、このように暗号化 U I D が書き込まれた R F タグ 1 5 0 は、各利用者に配布される。なお、ユーザ領域 1 5 0 b の意味については第 1 の実施の形態と同様である。

R F タグの利用：

発行された R F タグ 1 5 1 を取得した利用者は、この R F タグ 1 5 1 に格納されている E (P K_i, U I D_j) を R F タグ読み取り部 1 2 1 d によって読み取らせる (ステップ S 4 0) 。 R F タグ読み取り部 1 2 1 d によって読み取られた E (P K_i, U I D_j) は、復号部 1 2 1 e に送られ、復号部 1 2 1 e は、鍵情報記憶部 1 2 1 b に記憶されている R F タグ利用装置 1 2 1 の秘密鍵 S K_i を抽出する。そして、この暗号部 1 2 1 e は、抽出した秘密鍵 S K_i を用いて受け取った E (P K_i, U I D_j) を復号し (D (S K_i, E (P K_i, U I D_j)) し、その結果 U I D_j をタグ情報抽出部 1 2 1 g に送る (ステップ S 4 1) 。タグ情報抽出部 1 2 1 g では、第 1 の実施の形態と同様に、送られた U I D_j に対応する商品 I D (P I D_j) を U I D データ記憶部 1 2 1 f から抽出し、出力する (ステップ S 4 2) 。

10

【 0 0 3 1 】

このように、この形態の R F タグ発行装置 1 1 0 では、固有 I D 情報入力手段となる通信部 1 1 1 において、非接触型の R F タグ 1 5 0 に格納する固有 I D 情報 (U I D_j) の入力を受け、固有 I D 情報変換手段である暗号化部 1 1 3 において、この入力された U I D_j を、所定の情報を用いなければ読解が困難な情報 (変換固有 I D 情報) である暗号化 U I D (E (P K_i, U I D_j)) に変換し、変換固有 I D 情報書き込み手段である U I D 書き込み部 1 1 4 において、この変換された暗号化 U I D (E (P K_i, U I D_j)) を、非接触型の R F タグ 1 5 0 に書き込むこととした。

20

そのため、R F タグ 2 5 0 の情報を読み取り、U I D として利用できる主体を、復号に必要な鍵を所有しているものに限定できる。つまり、このように発行された R F タグ 1 5 0 の内容を悪意の者が読み取ったとしても、この者が知り得る情報は暗号化 U I D (E (P K_i, U I D_j)) のみであり、この者は U I D 自体の内容を知ることができない。その結果、R F タグ 1 5 0 の U I D の内容が第三者に読み取られ、商品所有者のプライバシーが侵害されることもない。

【 0 0 3 2 】

また、第三者は、R F タグ 1 5 0 に格納された U I D の内容を読み取ることができないため、この U I D と商品の対応から特定の商品の U I D を推測することも容易ではない。その結果、U I D の偽造をも防止することができる。

30

さらに、暗号化 U I D (E (P K_i, U I D_j)) 自体は秘密情報でないため、R F タグ 1 5 0 に秘密情報を保持するための構造や、認証処理を行うための I C を必要とせず、R F タグ 1 5 0 のコストも安い。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態では、R F タグ利用装置 1 2 1 からネットワーク 1 4 0 を介して送られた U I D を、通信部 1 1 1 によって受信することにより、R F タグ発行装置 1 1 0 に U I D を入力することとしたが、R F タグ発行装置 1 1 0 に直接 U I D を入力することとしてもよい。

40

【 0 0 3 3 】

〔第 3 の実施の形態〕

この形態は、U I D を所定の乱数を対応づけ、この乱数を R F タグに格納する形態である。なお、第 1 の実施の形態と共通する事項については説明を省略する。

図 1 4 は、図 2 の (a) と同様なハードウェア構成において所定のプログラムを実行させることによって構成される R F タグ発行装置 2 1 0 の機能構成の例示であり、図 1 5 は、乱数情報記憶部 2 1 0 c に格納された乱数情報 1 0 1 1 のデータ構成を例示した図であり、図 1 6 は、R F タグ 2 5 0 のデータ構成の例示であり、図 1 7 は、図 2 の (b) と同様なハードウェア構成において所定のプログラムを実行させることによって構成される R F タグ利用装置 2 2 0 の機能構成の例示である。また、図 1 8 の (a) (c) は、R F タグ発行装置 2 1 0 の処理を説明するためのフローチャートであり、(b) は、R F タグ利用

50

装置 2 2 0 の処理を説明するためのフローチャートである。

【 0 0 3 4 】

以下、これらの図を用いて、本形態における R F タグ発行装置 2 1 0 及び R F タグ利用装置 2 2 0 の機能構成及び処理について説明を行っていく。なお、システムの全体構成については、例えば、第 1 の実施の形態と同様のものとする。また、R F タグ発行装置 2 1 0 の制御は制御部 2 1 0 j によって、R F タグ利用装置 2 2 0 の制御は制御部 2 2 5 によって行われる。

R F タグの発行：

まず、R F タグの発行の前提として、R F タグ発行装置 2 1 0 の利用者情報入力部 2 1 0 a から利用者情報 (C I_i) の入力を受け付ける (ステップ S 5 0)。入力された利用者情報 (C I_i) は利用者 I D 生成部 2 1 0 b に送られ、利用者 I D 生成部 2 1 0 b は、これに対応する利用者 I D (C I D_i) を生成する。生成された利用者 I D (C I D_i) は、乱数情報記憶部 2 1 0 c に送られ、そこで記憶される (ステップ S 5 1)。

【 0 0 3 5 】

この記憶された利用者 I D (C I D_i) は、利用者 I D 出力部 2 1 0 d によって抽出・出力され (ステップ S 5 2)、各利用者に配布される。また、この出力された利用者 I D (C I D_i) は、書き込まれる U I D (U I D_j) とともに U I D 入力部 2 1 0 e から入力され、乱数情報生成部 2 1 0 f に送られる (ステップ S 5 3)。

利用者 I D (C I D_i) と U I D (U I D_j) を受け取った乱数情報生成部 2 1 0 f は、乱数発生部 2 1 0 f a によって発生させた乱数 (R_j) を取得し、これら利用者 I D (C I D_i)、U I D (U I D_j)、及び乱数 (R_j) の対応付けを行う。このように対応付けられた利用者 I D (C I D_i)、U I D (U I D_j)、及び乱数 (R_j) は、乱数情報記憶部 2 1 0 c に送られ、そこで記録される (ステップ S 5 4)。

【 0 0 3 6 】

ここで、これらの利用者 I D (C I D_i) 1 0 1 1 a、U I D (U I D_j) 1 0 1 1 d、及び乱数 (R_j) 1 0 1 1 c は、例えば、利用者情報 (C I_i) 1 0 1 1 b に対応付けられた乱数情報 1 0 1 1 として格納される (図 1 5)。図 1 5 の例の場合、利用者 I D 「A A 1 1 1 1 1」に対して、乱数「3 2 1 6 5 4」と U I D 「1 2 3 4 5 6」の組み合わせ、及び乱数「6 5 4 7 8 9」と U I D 「2 3 4 5 6 7」の組み合わせが対応付けられ、利用者 I D 「A A 1 1 1 1 1 2」に対して、乱数「7 4 1 2 5 8」と U I D 「9 8 7 6 5 4」の組み合わせが、利用者 I D 「A A 1 1 1 1 1 3」に対して、乱数「3 6 9 8 5 2」と U I D 「8 7 4 5 6 3」の組み合わせ、及び乱数「4 8 7 5 3 2」と U I D 「7 4 1 2 3 6」の組み合わせが対応付けられている。

【 0 0 3 7 】

その後、乱数情報生成部 2 1 0 f は、この U I D に対応付けられた乱数 (R_j) を U I D 書き込み部 2 1 0 g に送り、U I D 書き込み部 2 1 0 g は、この乱数 (R_j) を R F タグ 2 5 0 の乱数領域 2 5 1 に書きこむ (図 1 6) (ステップ S 5 5)。なお、R F タグ 2 5 0 のユーザ領域 2 5 2 の意味は、第 1 の実施の形態と同様である。そして、このように乱数

R F タグの利用：

発行された R F タグ 2 5 0 を取得した利用者は、まず、R F タグ利用装置 2 2 0 に自己の利用者 I D (C I D_i) を入力する。この利用者 I D (C I D_i) は、利用者 I D 入力部 2 2 1 に入力され、通信部 2 2 3 に送られる (ステップ S 6 0)。また、利用者は、R F タグ 2 5 0 に格納されている乱数 (R_j) を R F タグ読み取り部 2 2 2 によって読み取らせる (ステップ S 4 0)。R F タグ読み取り部 1 2 1 d によって読み取られた乱数 (R_j) も通信部 2 2 3 に送られ、通信部は、この乱数 (R_j) と利用者 I D (C I D_i) とをネットワーク 2 4 0 を介し、R F タグ発行装置 2 1 0 に送信する (ステップ S 6 2)。

【 0 0 3 8 】

送信された乱数 (R_j) と利用者 I D (C I D_i) は、R F タグ発行装置 2 1 0 の通信部 2 1 0 h で受信され復元部 2 1 0 i に送られる (ステップ S 7 0)。復元部 2 1 0 i で

は、この乱数 (R_j) と利用者 ID (CID_j) とに関連付けられている UID (UID_j) を乱数情報記憶部 210c の乱数情報 1011 から抽出し、UID (UID_j) の復元を行う (ステップ S71)。このように復元された UID (UID_j) は通信部 210h に送られ、そこからネットワーク 240 を通じて RF タグ利用装置 220 に送信される (ステップ S72)。

送信された UID (UID_j) は、RF タグ利用装置 220 の通信部 223 によって受信され (ステップ S63)、タグ情報抽出部 225 に送られる。タグ情報抽出部 225 では、第 1 の実施の形態と同様、送られた UID (UID_j) に対応する商品 ID (PID_k) から抽出し、出力する (ステップ S64)。

【0039】

このように、この形態の RF タグ発行装置 210 では、固有 ID 情報入力手段である UID 入力部 210e において、非接触型の RF タグ 250 に格納する固有 ID 情報 (UID_j) の入力を受け、固有 ID 情報変換手段である乱数情報生成部 210f において、この入力された UID_j を、所定の情報を用いなければ読解が困難な情報 (変換固有 ID 情報) である乱数 (R_j) に変換し、変換固有 ID 情報書き込み手段である UID 書き込み部 210g において、この変換された乱数 (R_j) を、非接触型の RF タグ 250 に書き込むこととした。

そのため、RF タグ 250 の情報を読み取り、UID として利用できる主体を、UID_j と乱数 (R_j) との対応関係を知っているものに限定することができる。つまり、このように発行された RF タグ 250 の内容を悪意の者が読み取ったとしても、この者が知り得る情報は乱数 (R_j) のみであり、この者は UID 自体の内容を知ることができない。その結果、RF タグ 250 の UID の内容が第三者に読み取られ、商品所有者のプライバシーが侵害されることもない。

【0040】

また、第三者は、RF タグ 250 に格納された UID の内容を読み取ることができないため、この UID と商品の対応から特定の商品の UID を推測することも容易ではない。その結果、UID の偽造をも防止することができる。

さらに、乱数 (R_j) 自体は秘密情報でないため、RF タグ 250 に秘密情報を保持するための構造や、認証処理を行うための IC を必要とせず、RF タグ 250 のコストも安い。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態において、第 1 の実施の形態と同様な決済処理を付加した構成としてもよい。

【0041】

〔第 4 の実施の形態〕

この形態は、UID とともにデジタル署名を RF タグに格納する形態である。なお、第 1 の実施の形態と共通する事項については説明を省略する。また、この形態のデジタル署名に使用する暗号化アルゴリズムは、RSA 等特に制限はなく、RF タグ発行装置、RF タグ利用装置間において、予め取決め・設定しておくものとする。

図 19 は、図 2 の (a) と同様なハードウェア構成において所定のプログラムを実行させることによって構成される RF タグ発行装置 310 の機能構成の例示であり、図 20 は、RF タグ 350 のデータ構成の例示であり、図 21 は、図 2 の (b) と同様なハードウェア構成において所定のプログラムを実行させることによって構成される RF タグ利用装置 320 の機能構成の例示である。また、図 22 の (a) は、RF タグ発行装置 310 の処理を説明するためのフローチャートであり、(b) は、RF タグ利用装置 320 の処理を説明するためのフローチャートである。

【0042】

以下、これらの図を用いて、本形態における RF タグ発行装置 310 及び RF タグ利用装置 320 の機能構成及び処理について説明を行っていく。なお、システムの全体構成については、例えば、第 1 の実施の形態と同様のものとする。また、RF タグ発行装置 310 の制御は制御部 315 によって、RF タグ利用装置 320 の制御は制御部 226 によって

行われる。

RFタグの発行：

まず、RFタグ発行装置310のUID入力部311においてUID (UID_j) の入力を受け付け (ステップS81)、入力されたUID (UID_j) を署名部313に送る。署名部313では、鍵情報記憶部312に格納されているRFタグ発行装置310の秘密鍵SK_iを抽出し、この秘密鍵SK_iを用いて署名 (Sig SK_i (UID_j)) を生成する (ステップS82)。生成された署名 (Sig SK_i (UID_j)) とUID (UID_j) はUID書き込み部83に送られ、そこでRFタグ350のUDI領域351にUID (UID_j) が、署名領域352に署名 (Sig SK_i (UID_j)) が、それぞれ書き込まれる (図20) (ステップS83)。なお、ユーザ領域353の意味は、第1の実施の形態と同様である。そして、このように署名とUIDが書き込まれたRFタグ350は、各利用者に配布される。

【0043】

RFタグの利用：

発行されたRFタグ350を取得した利用者は、このRFタグ350の署名 (Sig SK_i (UID_j)) とUID (UID_j) をRFタグ利用装置320のRFタグ読み取り部321に読み取らせる (ステップS91)。読み取られた署名 (Sig SK_i (UID_j)) とUID (UID_j) は署名検証部322に送られ、そこで署名の検証が行われる。すなわち、公開鍵記憶部323から、そこに記憶しておいたRFタグ発行装置310の秘密鍵SK_iに対応する公開鍵PK_iを抽出し、Verify PK_i (E (SK_i, UID_j)) = OK or NGを検証する (ステップS92)。ここで、NGとなれば、署名を拒否する旨の信号をタグ情報抽出部324に送って処理を終了し (ステップS93)、OKとなれば、署名を受諾する旨の信号をタグ情報抽出部324に送る。

【0044】

署名を受諾する旨の信号を受け取ったタグ情報抽出部324は、RFタグ読み取り部321からUID (UID_j) を受け取り、第1の実施の形態と同様に、このUID (UID_j) に対応する商品ID (PID_k) をUIDデータ記憶部325から抽出して出力する (ステップS94)。

このように、この形態のRFタグ発行装置310では、改ざん防止情報生成手段である署名部313において、固有ID情報の改ざんを防止するための改ざん防止情報である署名 (Sig SK_i (UID_j)) を生成し、改ざん防止情報書き込み手段に相当するUID書き込み部314において、この署名 (Sig SK_i (UID_j)) を非接触型のRFタグ350に書き込むこととした。そのため、RFタグ350の内容が偽造されたとしても、この署名を検証することにより、容易にその偽造を発見することができる。

【0045】

なお、この発明は上述の実施の形態に限定されるものではない。

〔第5の実施の形態〕

この形態は、UIDとともにメッセージ認証子 (MAC) をRFタグに格納する形態である。なお、第1の実施の形態と共通する事項については説明を省略する。なお、この形態で使用するMACアルゴリズムは、特に制限はなく、RFタグ発行装置、RFタグ利用装置間において、予め取決め・設定しておくものとする。

図23は、図2の (a) と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるRFタグ発行装置410の機能構成の例示であり、図24は、RFタグ450のデータ構成の例示であり、図25は、図2の (b) と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるRFタグ利用装置420の機能構成の例示である。また、図26の (a) は、RFタグ発行装置410の処理を説明するためのフローチャートであり、(b) は、RFタグ利用装置420の処理を説明するためのフローチャートである。

【0046】

以下、これらの図を用いて、本形態におけるRFタグ発行装置410及びRFタグ利用装

置 4 2 0 の機能構成及び処理について説明を行っていく。なお、システムの全体構成については、例えば、第 1 の実施の形態と同様のものとする。また、RF タグ発行装置 4 1 0 の制御は制御部 4 1 5 によって、RF タグ利用装置 4 2 0 の制御は制御部 4 2 6 によって行われる。

RF タグの発行：

まず、RF タグ発行装置 4 1 0 の UID 入力部 4 1 1 において UID (UID_i) の入力を受け付け (ステップ S 1 0 1)、入力された UID (UID_i) を MAC 演算部 4 1 3 に送る。この MAC 演算部 4 1 3 では、鍵情報記憶部 4 1 2 に格納されている MAC 用の秘密鍵 SK_i を抽出し、この秘密鍵 SK_i を用いて $MAC(h(SK_i, UID_i))$ を演算する (ステップ S 1 0 2)。なお、 h は RF タグ利用装置 4 2 0 と共用するハッシュ関数を意味し、 $h(a, b)$ は、鍵 a を用い、 b のハッシュ値を求めることを意味する。

【0047】

生成された $MAC(h(SK_i, UID_i))$ 及び UID (UID_i) は、UID 書き込み部 4 1 4 に送られ、そこで RF タグ 4 5 0 の UDI 領域 4 5 1 に UID (UID_i) が、MAC 領域 4 5 2 に $MAC(h(SK_i, UID_i))$ が、それぞれ書き込まれる (図 2 4) (ステップ S 1 0 3)。なお、ユーザ領域 4 5 3 の意味は、第 1 の実施の形態と同様である。そして、このように UID と MAC が書き込まれた RF タグ 4 5 0 は、各利用者に配布される。

RF タグの利用：

発行された RF タグ 3 5 0 を取得した利用者は、この RF タグ 3 5 0 の $MAC(h(SK_i, UID_i))$ と UID (UID_i) を RF タグ利用装置 4 2 0 の RF タグ読み取り部 4 2 1 に読み取らせる (ステップ S 1 1 1)。読み取られた $MAC(h(SK_i, UID_i))$ と UID (UID_i) は MAC 検証部 4 2 2 に送られ、そこで MAC の検証が行われる。すなわち、鍵情報記憶部 4 2 3 から、そこに記憶しておいた MAC 用の秘密鍵 SK_i' を抽出し、 $h(SK_i', UID_i) = h(SK_i, UID_i)$ となるか否かを検証する (ステップ S 1 1 2)。ここで、 $h(SK_i', UID_i) = h(SK_i, UID_i)$ とならなければ、この MAC を拒否する旨の信号をタグ情報抽出部 4 2 4 に送って処理を終了し (ステップ S 1 1 3)、 $h(SK_i', UID_i) = h(SK_i, UID_i)$ となれば、MAC を受諾する旨の信号をタグ情報抽出部 4 2 4 に送る。

【0048】

MAC を受諾する旨の信号を受け取ったタグ情報抽出部 4 2 4 は、RF タグ読み取り部 4 2 1 から UID (UID_i) を受け取り、第 1 の実施の形態と同様に、この UID (UID_i) に対応する商品 ID (PID_k) を UID データ記憶部 4 2 5 から抽出して出力する (ステップ S 1 1 4)。

このように、この形態の RF タグ発行装置 4 1 0 では、改ざん防止情報生成手段である MAC 演算部 4 1 3 において、固有 ID 情報の改ざんを防止するための改ざん防止情報である $MAC(h(SK_i, UID_i))$ を生成し、改ざん防止情報書き込み手段に相当する UID 書き込み部 4 1 4 において、この $MAC(h(SK_i, UID_i))$ を非接触型の RF タグ 4 5 0 に書き込むこととした。そのため、RF タグ 4 5 0 の内容が偽造されたとしても、この MAC を検証することにより、容易にその偽造を発見することができる。

【0049】

なお、この発明は上述の実施の形態に限定されるものではない。

〔第 6 の実施の形態〕

この形態は、UID を暗号化して RF タグに書き込み、さらにこの暗号化された UID とともにデジタル署名を RF タグに格納する形態である。なお、この形態の例では、公開鍵暗号方式を用いて暗号化、及びデジタル署名の付与を行う。また、使用する暗号化アルゴリズムについては特に制限はないが、RF タグ発行装置、RF タグ利用装置間において、予め取決め・設定しておくものとする。

図 2 7 は、図 2 の (a) と同様なハードウェア構成において所定のプログラムを実行させることによって構成される RF タグ発行装置 5 1 0 の機能構成の例示であり、図 2 8 は、

30

40

50

R F タグ 5 5 0 のデータ構成の例示であり、図 2 9 は、図 2 の (b) と同様なハードウェア構成において所定のプログラムを実行させることによって構成される R F タグ利用装置 5 2 0 の機能構成の例示である。また、図 3 0 の (a) 及び図 3 1 は、R F タグ発行装置 5 1 0 の処理を説明するためのフローチャートであり、図 3 0 の (b) は、R F タグ利用装置 5 2 0 の処理を説明するためのフローチャートである。

【 0 0 5 0 】

以下、これらの図を用いて、本形態における R F タグ発行装置 5 1 0 及び R F タグ利用装置 5 2 0 の機能構成及び処理について説明を行っていく。なお、システムの全体構成については、例えば、第 2 の実施の形態と同様のものとする。また、R F タグ発行装置 5 1 0 の制御は制御部 5 1 7 によって、R F タグ利用装置 5 2 0 の制御は制御部 5 2 0 i によっ 10 て行われる。

R F タグの発行：

まず、R F タグ利用装置 5 2 0 の U I D 入力部 5 2 0 a において、U I D_jの入力を受け付け、入力された U I D_jを通信部 5 2 0 c に送る (ステップ S 1 2 1)。また、ネットワーク 5 4 0 を介して認証局装置から取得し、鍵情報記憶部 5 2 0 b に記憶されている公開鍵証明書 (C e r t P K_i (P K_i)) を読み出し、通信部 5 2 0 c に送る。これらの情報が送られた通信部 5 2 0 c は、これらの U I D_j及び公開鍵証明書 (C e r t P K_i (P K_i)) を、ネットワーク 5 4 0 を介し、R F タグ発行装置 5 1 0 に送る (ステップ S 1 2 2)。なお、S K_iは認証局装置の秘密鍵を、P K_iは R F タグ利用装置 5 2 0 の公開鍵を意味する。 20

【 0 0 5 1 】

これらの情報が送られた R F タグ発行装置 5 1 0 は、通信部 5 1 1 によって、これら (U I D_j, C e r t P K_i (P K_i)) を受信する。また、通信部 5 1 1 は、ネットワーク 5 4 0 を介し、認証局装置から認証局装置の公開鍵 P K_iを取得する (ステップ S 1 3 1)。

通信部 5 1 1 に受信された公開鍵証明書 (C e r t P K_i (P K_i)) 及び認証局装置の公開鍵 P K_iは、公開鍵検証部 5 1 2 に送られ、この公開鍵検証部 5 1 2 は、(V e r i f y P K_i (C e r t P K_i (P K_i))) = O K o r N G を検証する (ステップ S 1 3 2)。ここで、N G となれば、公開鍵 P K_iを拒否する旨の信号を暗号化部 5 1 3 に送って処理を終了し (ステップ S 3 2)、O K となれば、公開鍵 P K_iを受諾する旨の信号を暗号化部 5 1 3 に送り、暗号化部 5 1 3 は、通信部 5 1 1 から U I D_jと公開鍵 P K_iを取得し、この公開鍵 P K_iで U I D_jを暗号化 (E (P K_i, U I D_j)) する (ステップ S 1 3 4)。 30

【 0 0 5 2 】

このように暗号化された E (P K_i, U I D_j) (暗号化 U I D) は、署名部 5 1 4 に送られ、署名部 5 1 4 では、鍵情報記憶部 5 1 5 に格納されている R F タグ発行装置 5 1 0 の秘密鍵 S K_nを抽出し、この秘密鍵 S K_nを用いて署名 (S i g S K_n (E (P K_i, U I D_j))) を生成する (ステップ S 1 3 5)。生成された署名 (S i g S K_n (E (P K_i, U I D_j))) と、暗号化 U I D (E (P K_i, U I D_j)) は、U I D 書き込み部 5 1 6 に送られ、そこで R F タグ 5 5 0 の暗号化 U D I 領域 5 5 1 に暗号化 U I D (E (P K_i, U I D_j)) が、署名領域 5 5 2 に署名 (S i g S K_n (E (P K_i, U I D_j))) が、それぞれ書き込まれる (図 2 8) (ステップ S 1 3 6)。なお、ユーザ領域 5 5 3 の意味は、第 1 の実施の形態と同様である。そして、このように暗号化 U I D 及び署名が書き込まれた R F タグ 5 5 0 は、各利用者に配布される。 40

【 0 0 5 3 】

R F タグの利用：

発行された R F タグ 5 5 0 を取得した利用者は、この R F タグ 5 5 0 の署名 (S i g S K_n (E (P K_i, U I D_j))) と暗号化 U I D (E (P K_i, U I D_j)) を R F タグ利用装置 5 2 0 の R F タグ読み取り部 5 2 0 d に読み取らせる (ステップ S 1 4 1)。読み取られた署名 (S i g S K_n (E (P K_i, U I D_j))) と暗号化 U I D (E (50

$PK_i, UID_j)$ は署名検証部 520e に送られ、そこで署名の検証が行われる。すなわち、鍵情報記憶部 520b から、そこに記憶しておいた RF タグ発行装置 510 の秘密鍵 SK_h に対応する公開鍵 PK_h を抽出し、 $Verify\ PK_h(E(SK_h, E(PK_i, UID_j))) = OK\ or\ NG$ を検証する (ステップ S142)。ここで、NG となれば、署名を拒否する旨の信号を復号部 520f に送って処理を終了し (ステップ S143)、OK となれば、署名を受諾する旨の信号を復号部 520f に送る。

【0054】

署名を受諾する旨の信号を受け取った復号部 520f は、RF タグ読み取り部 520d から暗号化 $UID(E(PK_i, UID_j))$ を受け取り、さらに鍵情報記憶部 520b から公開鍵 PK_i に対応する秘密鍵 SK_i を抽出して、暗号化 $UID(E(PK_i, UID_j))$ を復号 ($D(SK_i, E(PK_i, UID_j))$) する (ステップ S144)。その復号結果である $UID(UID_j)$ は、タグ情報抽出部 520g に送られ、タグ情報抽出部 520g は、第 1 の実施の形態と同様に、この $UID(UID_j)$ に対応する商品 ID (PID_k) を UID データ記憶部 520h から抽出して出力する (ステップ S145)。

このように、この形態の RF タグ発行装置 510 では、固有 ID 情報入力手段となる通信部 511 において、非接触型の RF タグ 550 に格納する固有 ID 情報 (UID_j) の入力を受け、固有 ID 情報変換手段である暗号化部 513 において、この入力された UID_j を、所定の情報を用いなければ読解が困難な情報 (変換固有 ID 情報) である暗号化 $UID(E(PK_i, UID_j))$ に変換し、変換固有 ID 情報書き込み手段である UID 書き込み部 514 において、この変換された暗号化 $UID(E(PK_i, UID_j))$ を、非接触型の RF タグ 550 に書き込むこととした。

【0055】

そのため、このように発行された RF タグ 550 の内容を悪意の者が読み取ったとしても、この者が知り得る情報は暗号化 $UID(E(PK_i, UID_j))$ のみであり、この者は UID 自体の内容を知ることができない。その結果、RF タグ 550 の UID の内容が第三者に読み取られ、商品所有者のプライバシーが侵害されることもない。

また、第三者は、RF タグ 550 に格納された UID の内容を読み取ることができないため、この UID と商品の対応から特定の商品の UID を推測することも容易ではない。その結果、 UID の偽造をも防止することができる。

さらに、暗号化 $UID(E(PK_i, UID_j))$ 自体は秘密情報でないため、RF タグ 550 に秘密情報を保持するための構造や、認証処理を行うための IC を必要とせず、RF タグ 550 のコストも安い。

【0056】

また、この形態の RF タグ発行装置 510 では、改ざん防止情報生成手段である署名部 514 において、固有 ID 情報の改ざんを防止するための改ざん防止情報である署名 ($Sig\ SK_h(E(PK_i, UID_j))$) を生成し、改ざん防止情報書き込み手段に相当する UID 書き込み部 516 において、この署名 ($Sig\ SK_h(E(PK_i, UID_j))$) を非接触型の RF タグ 550 に書き込むこととした。そのため、RF タグ 550 の内容が偽造されたとしても、この署名を検証することにより、容易にその偽造を発見することができる。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態では、RF タグ利用装置 520 からネットワーク 540 を介して送られた UID を、通信部 511 によって受信することにより、RF タグ発行装置 510 に UID を入力することとしたが、RF タグ発行装置 510 に直接 UID を入力することとしてもよい。また、この形態では公開鍵暗号方式を用いて UID の暗号化を行い、デジタル署名を付することとしたが、共通鍵暗号方式を用いて UID の暗号化を行うこととしてもよく、デジタル署名の代わりに MAC による認証を行う構成としてもよい。さらに、第 3 の実施の形態のように、 UID の暗号化の代わりに UID を乱数に置き換えることとしてもよい。

【0057】

〔第 7 の実施の形態〕

この形態は、第 2 の実施の形態の変形例であり、RF タグに複数の暗号化された U I D を書き込む形態である。つまり、第 2 の実施の形態では、RF タグ発行装置において、1 つの RF タグに対し、1 つの RF タグ利用装置から 1 つの U I D と 1 つの公開鍵を取得し、この公開鍵を用いて暗号化した 1 つの暗号化 U I D を書き込むこととしていた。これに対し、この形態では、RF タグ発行装置において、1 つの RF タグに対し、2 つの RF タグ利用装置から U I D と公開鍵をそれぞれ 1 つずつ取得し、取得した 2 つの U I D をそれぞれに対応する公開鍵で暗号化した 2 つの暗号化 U I D を書き込む形態である。

【 0 0 5 8 】

図 3 2 は、このように暗号化 U I D が格納された RF タグ 6 0 0 のデータ構成を例示した 10 図である。

この図に例示するように、この暗号化 U I D 領域 6 0 1 には、第 1 の RF タグ利用装置から提供された U I D₁ を、この第 1 の RF タグ利用装置の公開鍵 P K₁ で暗号化した暗号化 U I D (E (P K₁, U I D₁)) が格納され、暗号化 U I D 領域 6 0 2 には、第 2 の RF タグ利用装置から提供された U I D₂ を、この第 2 の RF タグ利用装置の公開鍵 P K₂ で暗号化した暗号化 U I D (E (P K₂, U I D₂)) が格納される。なお、システム構成及び処理動作については第 2 の実施の形態と同様であり、ユーザ領域 6 0 3 の意味については第 1 の実施の形態と同様であるため、ここでは説明を省略する。

【 0 0 5 9 】

このように暗号 U I D が格納された RF タグ 6 0 0 は、例えば、所定の利用者に配布され 20、そこで所定の商品等に付されて市場を流通する。流通過程においてこの RF タグ 6 0 0 を取得した利用者（仲介業者等）は、自己の秘密鍵を用いて、この RF タグ 6 0 0 に格納されている暗号化 U I D を復号する。この場合、この利用者が復号できるのは、自己が秘密鍵を知っている暗号化 U I D のみであり、その他の暗号化 U I D については復号できない。従って、この利用者は自己が秘密鍵を知っている暗号化 U I D の内容しか知ることができない。

このように、この形態では、固有 I D 情報入力手段（例えば、第 2 の実施の形態の通信部 1 1 1 が相当）において、複数の固有 I D 情報（U I D）の入力を受け付け、固有 I D 情報変換手段（例えば、第 2 の実施の形態の暗号化部 1 1 3 が相当）において、入力された 30 複数の U I D の少なくとも一部を、入力された他の U I D と異なる方法（異なる公開鍵 P K₁, P K₂）によって、変換固有 I D 情報に変換する（暗号化する）こととした。そのため、利用者は自己が秘密鍵を知っている暗号化 U I D の内容しか知ることができず、流通過程において RF タグが共用される場合であっても、自己の秘密情報が他の利用者に知られてしまうことはない。

【 0 0 6 0 】

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態では、U I D の暗号化に公開鍵暗号方式を利用したが、共通鍵暗号方式を利用してもよい。また、3 以上の U I D を複数の公開鍵を用いて暗号化して RF タグ 6 0 0 に書き込む構成としてもよい。さらに、デジタル署名を RF タグ 6 0 0 に格納する構成としてもよい。

〔第 8 の実施の形態〕

この形態は、暗号化された U I D、その暗号化のアルゴリズム及び鍵を特定するための鍵 I D を RF タグに書き込むものである。

【 0 0 6 1 】

図 3 3 の (a) は、図 2 の (a) と同様なハードウェア構成において所定のプログラムを実行させることによって構成される RF タグ発行装置 7 1 0 の機能構成の例示であり、図 3 3 の (b) は、図 2 の (b) と同様なハードウェア構成において所定のプログラムを実行させることによって構成される RF タグ利用装置 7 2 0 の機能構成の例示である。また、図 3 4 は、RF タグ発行装置 7 1 0 の暗号情報記憶部 7 1 2 に格納されるアルゴリズム情報 1 0 2 0 及び鍵情報 1 0 3 0 のデータ構成の例示であり、図 3 5 は、RF タグ利用装置 7 2 0 の暗号情報記憶部 7 2 3 に格納されるアルゴリズム情報 1 0 4 0 及び鍵情報 1 0 50

50のデータ構成の例示である。さらに、図36は、RFタグ750のデータ構成の例示であり、図37の(a)は、RFタグ発行装置710の処理を説明するためのフローチャートであり、(b)は、RFタグ利用装置720の処理を説明するためのフローチャートである。

【0062】

以下、これらの図を用いて、本形態におけるRFタグ発行装置710及びRFタグ利用装置720の機能構成及び処理について説明を行っていく。なお、システムの全体構成については、例えば、第1の実施の形態と同様のものとする。また、RFタグ発行装置710の制御は制御部715によって、RFタグ利用装置720の制御は制御部726によって行われる。

10

RFタグの発行：

まず、事前処理として、RFタグ発行装置710の暗号情報記憶部712にアルゴリズム情報1020及び鍵情報1030が(図34)、RFタグ利用装置720の暗号情報記憶部723にアルゴリズム情報1040及び鍵情報1050が(図35)、それぞれ格納される。

【0063】

ここで、この例のアルゴリズム情報1020は、RFタグ発行装置710においてUIDを暗号化する際に使用する複数の暗号化アルゴリズム(E_m)が、暗号化アルゴリズムID(EID_m)に対応付けられた情報である。この例では、 $EID_m = 001, 003, 003$ に対し、 $E_m = E_1, E_2, E_3$ がそれぞれ対応付けられている(図34)。また、この例の鍵情報1030は、RFタグ発行装置710においてUIDを暗号化する際に使用する複数の共通鍵(KI_i)が、共通鍵ID(KID_i)に対応付けられた情報である。この例では、 $KID_i = K001, K003, K003$ に対し、 $KI_i = KI_1, KI_2, KI_3$ がそれぞれ対応付けられている(図34)。

20

【0064】

さらに、この例のアルゴリズム情報1040は、RFタグ利用装置720においてUIDを復号する際に使用する複数の復号アルゴリズム(D_m)が、暗号化アルゴリズムID(EID_m)に対応付けられた情報である。この例では、 $EID_m = 001, 003, 003$ に対し、 $D_m = D_1, D_2, D_3$ がそれぞれ対応付けられている(図35)。また、この例の鍵情報1050は、RFタグ発行装置710の暗号情報記憶部712に格納された鍵情報と同じ、複数の共通鍵(KI_i)が、共通鍵ID(KID_i)に対応付けられた情報である。この例では、 $KID_i = K001, K003, K003$ に対し、 $KI_i = KI_1, KI_2, KI_3$ がそれぞれ対応付けられている(図35)。

30

【0065】

RFタグの発行を行う場合、まず、RFタグ発行装置710のUID入力部711においてUID(UID_j)の入力を受け付け、入力されたUID(UID_j)を暗号化部713に送る(ステップS151)。UID(UID_j)を受け取った暗号化部713は、暗号情報記憶部712から、暗号化に用いる一組の暗号化アルゴリズム(E_m)、暗号化アルゴリズムID(EID_m)、共通鍵(KI_i)及び共通鍵ID(KID_i)を抽出し、抽出した暗号化アルゴリズム(E_m)及び共通鍵(KI_i)を用い、UID(UID_j)を暗号化($E_m(KI_i, UID_j)$)する(ステップS152)。暗号化されたUID($E_m(KI_i, UID_j)$)、及びその暗号化に使用した抽出した暗号化アルゴリズム(E_m)及び共通鍵(KI_i)に対応する暗号化アルゴリズムID(EID_m)及び共通鍵ID(KID_i)はUID書き込み部714に送られ、UID書き込み部714は、それらをRFタグ750に書き込む(ステップS153)。図36の例では、暗号化アルゴリズム領域751に暗号化アルゴリズムID(EID_m)が、鍵ID領域752に共通鍵ID(KID_i)が、暗号化UID領域753に暗号化されたUID($E_m(KI_i, UID_j)$)が、それぞれ格納される。なお、ユーザ領域754の意味は第1の実施の形態と同様である。このような書き込みが行われたRFタグ750は各利用者に配布される。

40

【0066】

50

RFタグの利用：

利用者は、まず、RFタグ利用装置720のRFタグ読み取り部721にRFタグ750に格納されている暗号化アルゴリズムID (EID_m)、共通鍵ID (KID_i) 及び暗号化UID ($E_m(KI_i, UID_j)$) を読み取らせる (ステップS161)。

読み取られたこれらの情報は復号部722に送られ、復号部722は、受け取った暗号化アルゴリズムID (EID_m) 及び共通鍵ID (KID_i) にそれぞれ対応付けられている復号アルゴリズム (D_m) 及び共通鍵 (KI_i) を、暗号情報記憶部723に格納されているアルゴリズム情報1040及び鍵情報1050から抽出する (ステップS162)。これらを抽出した復号部722は、抽出した復号アルゴリズム (D_m) 及び共通鍵 (KI_i) を用い、受け取った暗号化UID ($E_m(KI_i, UID_j)$) を復号 ($D_m(KI_i, E_m(KI_i, UID_j))$) し (ステップS163)、その復号結果であるUID (UID_j) をタグ情報抽出部724に送る。

【0067】

UID (UID_j) を受け取ったタグ情報抽出部724は、第1の実施の形態と同様に、このUID (UID_j) に対応する商品ID (PID_k) をUIDデータ記憶部725から抽出して出力する (ステップS164)。

このように、この形態では、RFタグ発行装置710のUID書き込み部714 (復元ID情報書き込み手段に相当) において、暗号化UID ($E_m(KI_i, UID_j)$) (変換固有ID情報に相当) を読解可能とするために用いる復号アルゴリズム (D_m) 及び共通鍵 (KI_i) (復元情報に相当) に関連付けた暗号化アルゴリズムID (EID_m) 及び共通鍵ID (KID_i) (復元ID情報に相当) を、非接触型のRFタグ750に書き込むこととした。

【0068】

これにより、アルゴリズム情報1020、1040及び鍵情報1030、1050を、RFタグ発行装置710及びRFタグ利用装置720において保持しておけば、予め、RFタグ750の発行に用いる暗号化アルゴリズムや鍵を、RFタグ発行装置710—RFタグ利用装置720間において取決めておかなくても、このRFタグ750の発行・利用を行うことができる。そのため、限られたメンバーのみの閉じた環境だけではなく、不特定多数の利用者が使用するようなオープンな環境においても安全にRFタグを利用することが可能となる。

また、この形態では、RFタグ利用装置720の暗号情報記憶部723 (復元情報格納手段に相当) に、暗号化UID ($E_m(KI_i, UID_j)$) (変換固有ID情報に相当) を読解可能とするために用いる復号アルゴリズム (D_m) 及び暗号化鍵 (KI_i) (復元情報に相当) を、暗号化アルゴリズムID (EID_m) 及び暗号化鍵ID (KID_i) (復元ID情報に相当) に対応付けて格納しておき、復元ID情報読み取り手段であるRFタグ読み取り部721において、非接触型のRFタグ750から、暗号化アルゴリズムID (EID_m) 及び暗号化鍵ID (KID_i) を読み取り、復元情報抽出手段である復号部722において、この読み取られた暗号化アルゴリズムID (EID_m) 及び暗号化鍵ID (KID_i) を用い、暗号情報記憶部723から、この暗号化アルゴリズムID (EID_m) 及び暗号化鍵ID (KID_i) に対応する復号アルゴリズム (D_m) 及び暗号化鍵 (KI_i) を抽出し、変換固有ID情報読み取り手段であるRFタグ読み取り部721において、RFタグ750から、暗号化UID ($E_m(KI_i, UID_j)$) を読み取り、固有ID情報復元手段である復号部722において、抽出した復号アルゴリズム (D_m) 及び暗号化鍵 (KI_i) を用い、暗号化UID ($E_m(KI_i, UID_j)$) を復号 (読解可能なように変換) することとした。

【0069】

これにより、上述のように、限られたメンバーのみの閉じた環境だけではなく、不特定多数の利用者が使用するようなオープンな環境においても安全にRFタグを利用することが可能となる。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態では共

通鍵暗号方式によってU I Dを暗号化してR Fタグ7 5 0に格納することとしたが、その他の暗号方式や第3の実施の形態のような乱数の置き換えによってU I Dを変換し、R Fタグ7 5 0に格納することとしてもよい。

【第9の実施の形態】

この形態は、暗号化U I Dとともに、この復号処理当を行う装置へのアクセス情報をR Fタグに格納するものである。

【0070】

図38は、この形態におけるR Fタグ利用システム800の全体を例示した概念図である。

図38に例示するように、この例のR Fタグ利用システム800は、非接触型のR Fタグ 10 850を発行するR Fタグ発行装置810、このR Fタグ851～853の利用に用いる複数のR Fタグ利用装置821～823、及び暗号化U I Dの復号処理等を行う複数のI D管理局装置831～832によって構成され、R Fタグ利用装置821～823、及びI D管理局装置831～832は、物理的又は理論的に安全なネットワーク840によって、相互に通信可能なように構成されている。

【0071】

図39の(a)は、図2の(a)と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるR Fタグ発行装置810の機能構成の例示であり、図39の(b)は、図2の(b)と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるR Fタグ利用装置821の機能構成の例示であり、図4 20 0は暗号情報記憶部812に格納される暗号情報1060のデータ構成の例示であり、図41は、R Fタグ850のデータ構成の例示である。また、図42の(a)は、図2の(a)と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるI D管理局装置831の機能構成の例示であり、(b)は、管理情報記憶部831cに格納されるI D管理情報1070のデータ構成の例示である。さらに、図43の(a)は、R Fタグ発行装置810の処理を説明するためのフローチャートであり、(b)は、R Fタグ利用装置821及びI D管理局装置831の処理を説明するためのフローチャートである。

【0072】

以下、これらの図を用いて、本形態におけるR Fタグ発行装置810及びR Fタグ利用装置 30 821の機能構成及び処理について説明を行っていく。なお、ここでは、R Fタグ利用装置821及びI D管理局装置831を例にとって説明するが、その構成及び処理は、その他のR Fタグ利用装置822～822及びI D管理局装置832についても同様とする。また、R Fタグ発行装置810の制御は制御部815によって、R Fタグ利用装置821の制御は制御部821cによって、I D管理局装置831の制御は制御部831dによって行われる。

R Fタグの発行：

まず、事前処理として、R Fタグ発行装置810の暗号情報記憶部812に暗号情報1060が、I D管理局装置831の管理情報記憶部831cにI D管理情報1070が格納される。

【0073】

図40に例示するように、暗号情報1060は、I D管理局装置831～832にアクセスするためのアドレス等のアクセスI D (A I D_i) 1061、暗号、署名といった処理の種類1062、それに使用するアルゴリズム(E_i) 1063、及び鍵情報(K I_i) 1064が相互に関連付けられた情報である。この例では、A I D_i=0001に対して、種類「暗号」、E_i=DES、K I_i=0234が、A I D_i=0002に対して、種類「署名」、E_i=RSA、K I_i=1234が、それぞれ関連付けられている。

また、図42に例示するように、I D管理情報1070は、I D管理局装置831のアクセスI D (A I D_i) 1071、取り扱う処理の種類1072、そのアルゴリズム(D_i) 1073、及び鍵情報(K I_i) 1074が対応付けられて格納されている。なお、こ 50

のID管理情報の内容は、ID管理局装置831～832ごとに異なるものとする。

【0074】

RFタグ850の発行を行う場合、まず、RFタグ発行装置810のUID入力部811においてアクセスID (AID_i) とUID (UID_j) の入力を受け付ける (ステップS171)。入力されたアクセスID (AID_i) とUID (UID_j) は暗号化部813に送られ、暗号化部813は、このアクセスID (AID_i) に対応付けられているアルゴリズム (E_i) 及び鍵情報 (KI_i) を暗号情報記憶部812から抽出する。これらを抽出した暗号化部813は、受け取ったUID (UID_j) に対し、抽出したアルゴリズム (E_i) 及び鍵情報 (KI_i) を用いた処理を行う。この例ではアクセスIDとして $AID_i = 0001$ が入力され、UID (UID_j) を、アルゴリズム (E_i) 及び鍵情報 (KI_i) を用いて暗号化 ($E_i(KI_i, UID_j)$) する処理を行うものとする (ステップS172)。

【0075】

このように暗号化UID ($E_i(KI_i, UID_j)$) とアクセスID (AID_i) は、UID書き込む部814に送られ、UID書き込む部814は、RFタグ850のアクセスID領域にアクセスID (AID_i) を、暗号化UID領域852に暗号化されたUID ($E_i(KI_i, UID_j)$) を書き込む (ステップS173)。そして、このような情報が書き込まれたRFタグ850は各利用者に配布される。なお、ユーザ領域853の意味は第1の実施の形態と同様である。

RFタグの利用：

RFタグ851を受け取った利用者は、まず、RFタグ利用装置821のRFタグ読み取り部821aに、このRFタグ851に格納された暗号化UID ($E_i(KI_i, UID_j)$) とアクセスID (AID_i) を読み取らせる (ステップS181)。読み取られたこれらの情報は、通信部821bに送られ、通信部821bは、受け取ったアクセスID (AID_i) によって特定されるID管理局装置831に、暗号化UID ($E_i(KI_i, UID_j)$) とアクセスID (AID_i) とを送信する (ステップS182)。

【0076】

送信されたこれらの情報は、ネットワーク840を介してID管理局装置831に送られ、その通信部831aによって受信される (ステップS183)。通信部831aは、受信したこれらの情報を復号部831bに送り、復号部831bは、このアクセスID (AID_i) に関連付けられているアルゴリズム (D_i) と鍵情報 (KI_i) を管理情報記憶部831cのID管理情報1070から抽出する。これらを抽出した復号部831bは、抽出したアルゴリズム (D_i) と鍵情報 (KI_i) を用い、受信した暗号化UID ($E_i(KI_i, UID_j)$) を復号 ($D_i(KI_i, E_i(KI_i, UID_j))$) する (ステップS184)。その復号結果 (UID_j) は、通信部831aに送られ、通信部831aは、この復号結果であるUID (UID_j) を、ネットワーク840を通じ、元のRFタグ利用装置821に送信する (ステップS185)。

【0077】

送信されたUID (UID_j) は、RFタグ利用装置821の通信部821bによって受信され (ステップS186)、タグ情報抽出部821cに送られる。そして、このUID (UID_j) を受け取ったタグ情報抽出部821cは、第1の実施の形態と同様に、このUID (UID_j) に対応する商品ID (PID_k) をUIDデータ記憶部821dから抽出して出力する (ステップS187)。

このように、この形態のRF利用装置821は、復元ID情報読み取り手段であるRFタグ読み取り部821aによって、非接触型のRFタグ851から復元ID情報であるアクセスID (AID_i) を読み取り、変換固有ID情報出力手段である通信部821bにおいて、この読み取られたアクセスID (AID_i) によって特定されるアドレスを指定して、変換固有ID情報である暗号化UID ($E_i(KI_i, UID_j)$) を出力することとした。

【0078】

そのため、このアクセスID (AID_i) によって特定されるID管理局装置831に、この暗号化UID (E_i(KI_i, UID_i)) の復号に必要なアルゴリズム(D_i) と鍵情報(KI_i) をアクセスID (AID_i) に対応付けて格納しておくことにより、このID管理局装置831において、この暗号化UID (E_i(KI_i, UID_i)) の復号に必要なアルゴリズム(D_i) と鍵情報(KI_i) を導出し、その復号を行うことができる。従って、RFタグ発行者と利用者との間で予め使用するアルゴリズムや鍵情報の合意がなくても、その利用者はRFタグを復号することが可能となり、限られたメンバーのみの閉じた環境だけではなく、不特定多数の利用者が使用するようなオープンな環境においても安全にRFタグを利用することが可能となる。

【0079】

10

また、ヘッダ領域を設けず、通常UIDが書き込まれる領域をアクセスID領域851とした場合、この形態のタグ構成を通常のRFタグフォーマットによって実現することができる。この場合、RFタグのデータ読み込みのために、新たなプログラムを用意する必要がなくなる。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態の説明では、暗号処理に関連付けられたアクセスID (AID_i) が入力された場合を例にとって説明したが、署名処理に関連付けられたアクセスID (AID_i) が入力された場合であっても、その処理は、暗号化が署名生成に変わり、復号が署名検証に変わるのみであって同様である。

【0080】

20

また、上述の各実施の形態で説明したRFタグのフォーマットは単なる例示であり、これに限定されるものではない。例えば、ユーザ領域のないフォーマット、アクセス制御機能のついたフォーマット等を用いることとしてもよい。

さらに、上述の各実施の形態を組み合わせた構成をとることとしてもよい。

また、上述の各実施の形態では、コンピュータ上で所定のプログラムを実行させることにより、RFタグ発行装置、RFタグ利用装置、決済処理サーバ装置、認証局装置及びID管理局装置を構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

【0081】

さらに、上述のように、この形態のRFタグ発行装置、RFタグ利用装置、決済処理サーバ装置、認証局装置及びID管理局装置が有すべき機能の処理内容をプログラムに記述し、このプログラムをコンピュータで実行することにより、これらの処理機能をコンピュータ上で実現することができる。

なお、この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等のようなものでもよいが、具体的には、例えば、磁気記録装置として、ハードディスク装置、フレキシブルディスク、磁気テープ等を、光ディスクとして、DVD (Digital Versatile Disc)、DVD-RAM (Random Access Memory)、CD-ROM (Compact Disc Read Only Memory)、CD-R (40 Recordable) / RW (Rewritable) 等を、光磁気記録媒体として、MO (Magnetooptical disc) 等を、半導体メモリとしてEPROM (Erasable and Programmable ROM) 等を用いることができる。

【0082】

また、このプログラムの流通は、例えば、そのプログラムを記録したDVD、CD-ROM等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

50

このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理実行時、このコンピュータは、自己の記録媒体に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、コンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。

【 0 0 8 3 】

【 発 明 の 効 果 】

以上説明したように、この発明では、非接触型 R F タグに格納する固有 I D 情報の入力を受け付け、入力された固有 I D 情報を、所定の情報を用いなければ読解が困難な情報に変換し、この変換された変換固有 I D 情報を、非接触型の R F タグに書き込むこととしたため、低コストで、R F タグに格納された U I D の安全性を向上させ、その偽造を防止することが可能となる。

【 図 面 の 簡 単 な 説 明 】

【 図 1 】 R F タグ利用システムの全体を例示した概念図。

【 図 2 】 (a) は、図 1 に例示した R F タグ発行装置のハードウェア構成を例示したブロック図であり、(b) は、R F タグ利用装置のハードウェア構成を例示したブロック図である。

【 図 3 】 図 2 の (a) に例示したハードウェア構成において所定のプログラムを実行させることによって構成される R F タグ発行装置の機能構成の例示。

【 図 4 】 R F タグ発行装置の暗号情報記憶部に格納される暗号データベースのデータ構成を例示した図。

【 図 5 】 R F タグに格納されるデータの構成を例示した概念図。

【 図 6 】 R F タグ利用装置の機能構成を例示した図。

【 図 7 】 R F タグ利用装置に格納される U I D データベースの構成を例示した概念図。

【 図 8 】 (a) 及び (c) は、この例の R F タグ発行装置の処理を説明するためのフローチャートであり、(b) は、この例の R F タグ利用装置の処理を説明するためのフローチャートである。

【 図 9 】 R F タグ利用システムの全体を例示した概念図。

【 図 1 0 】 R F タグ発行装置の機能構成を例示した図。

【 図 1 1 】 R F タグのデータ構成を例示した図。

【 図 1 2 】 R F タグ利用装置の機能構成を例示した図。

【 図 1 3 】 (a) は、R F タグ発行装置の処理を説明するためのフローチャートであり、(b) は、R F タグ利用装置の処理を説明するためのフローチャートである。

【 図 1 4 】 R F タグ発行装置の機能構成を例示した図。

【 図 1 5 】 乱数情報記憶部に格納された乱数情報のデータ構成を例示した図。

【 図 1 6 】 R F タグのデータ構成を例示した図。

【 図 1 7 】 R F タグ利用装置の機能構成を例示した図。

【 図 1 8 】 (a) (c) は、R F タグ発行装置の処理を説明するためのフローチャートであり、(b) は、R F タグ利用装置の処理を説明するためのフローチャートである。

【 図 1 9 】 R F タグ発行装置の機能構成を例示した図。

【 図 2 0 】 R F タグのデータ構成を例示した図。

【 図 2 1 】 R F タグ利用装置の機能構成を例示した図。

【 図 2 2 】 (a) は、R F タグ発行装置の処理を説明するためのフローチャートであり、(b) は、R F タグ利用装置の処理を説明するためのフローチャートである。

【 図 2 3 】 R F タグ発行装置の機能構成を例示した図。

【 図 2 4 】 R F タグのデータ構成を例示した図。

【 図 2 5 】 R F タグ利用装置の機能構成を例示した図。

【図 26】 (a) は、RF タグ発行装置の処理を説明するためのフローチャートであり、(b) は、RF タグ利用装置の処理を説明するためのフローチャートである。

【図 27】 RF タグ発行装置の機能構成を例示した図。

【図 28】 RF タグのデータ構成を例示した図。

【図 29】 RF タグ利用装置の機能構成を例示した図。

【図 30】 (a) は、RF タグ発行装置の処理を説明するためのフローチャートであり、(b) は、RF タグ利用装置の処理を説明するためのフローチャートである。

【図 31】 RF タグ発行装置の処理を説明するためのフローチャート。

【図 32】 RF タグのデータ構成を例示した図。

【図 33】 (a) は、RF タグ発行装置の機能構成を例示した図であり、(b) は、RF 10 タグ利用装置の機能構成を例示した図である。

【図 34】 RF タグ発行装置の暗号情報記憶部に格納されるアルゴリズム情報及び鍵情報のデータ構成を例示した図。

【図 35】 RF タグ利用装置の暗号情報記憶部に格納されるアルゴリズム情報及び鍵情報のデータ構成を例示した図。

【図 36】 RF タグのデータ構成を例示した図。

【図 37】 (a) は、RF タグ発行装置の処理を説明するためのフローチャートであり、(b) は、RF タグ利用装置の処理を説明するためのフローチャートである。

【図 38】 RF タグ利用システムの全体を例示した概念図。

【図 39】 (a) は、RF タグ発行装置の機能構成を例示した図であり、(b) は、RF 20 タグ利用装置の機能構成を例示した図。

【図 40】 暗号情報記憶部に格納される暗号情報のデータ構成を例示した図。

【図 41】 RF タグのデータ構成を例示した図。

【図 42】 (a) は、ID 管理局装置の機能構成を例示した図であり、(b) は、管理情報記憶部に格納される ID 管理情報のデータ構成を例示した図である。

【図 43】 (a) は、RF タグ発行装置の処理を説明するためのフローチャートであり、(b) は、RF タグ利用装置及び ID 管理局装置の処理を説明するためのフローチャートである。

【符号の説明】

1、101、800 RF タグ利用システム

10、110、210、310、410、510、710、810 RF タグ発行装置

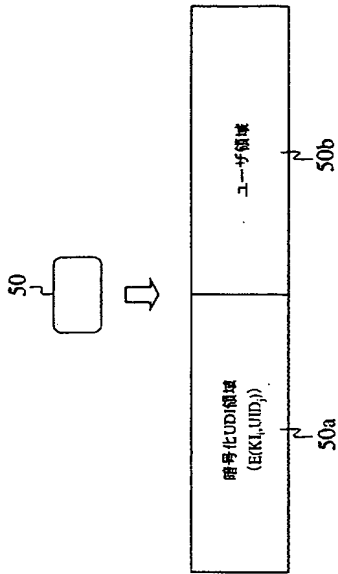
21～23、121～123、220、320、420、520、720、821～82

3 RF タグ利用装置

50～53、150～153、250、350、450、550、600、750、85

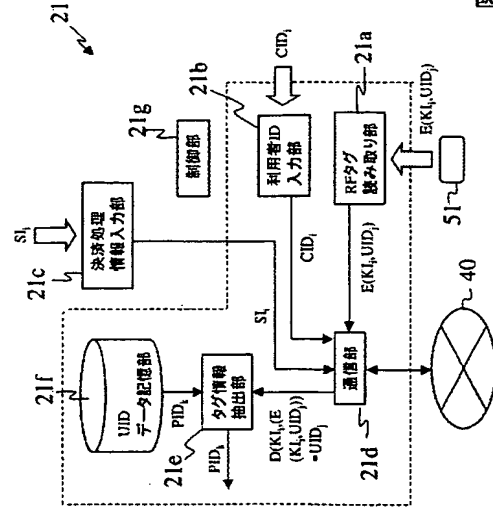
0～853 RF タグ

【 図 5 】



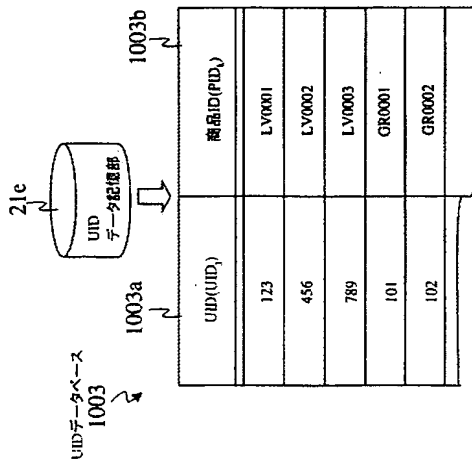
5

【 図 6 】



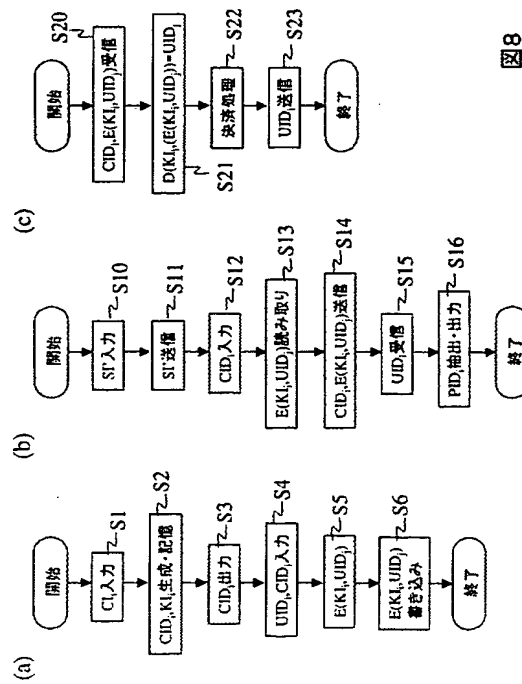
9

【 図 7 】



7. 図

【圖 8】



8

【 図 9 】

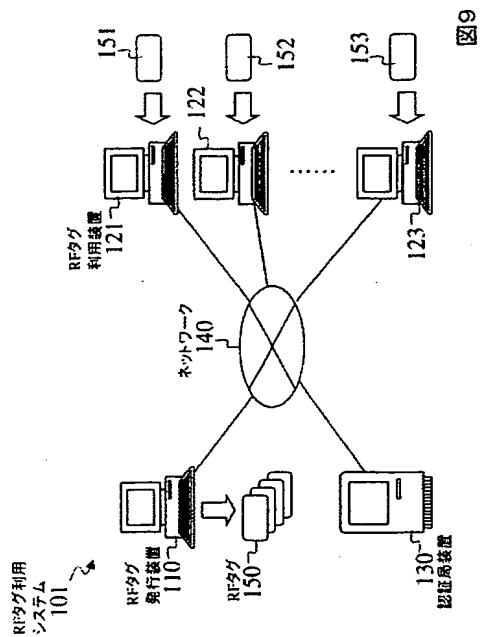


図9

【 図 10 】

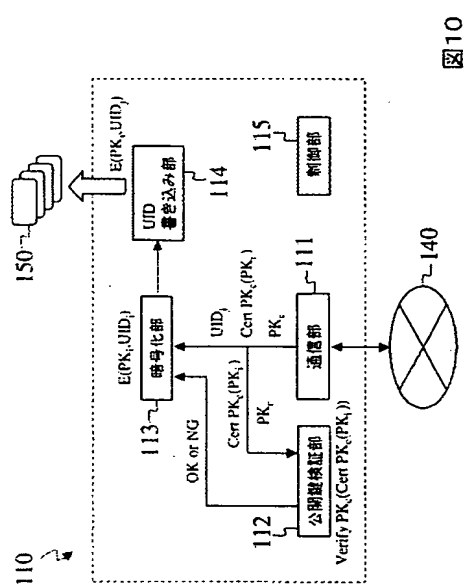


図10

【 図 11 】

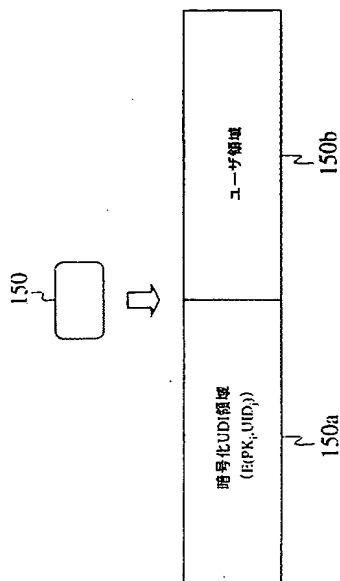


図11

【 図 12 】

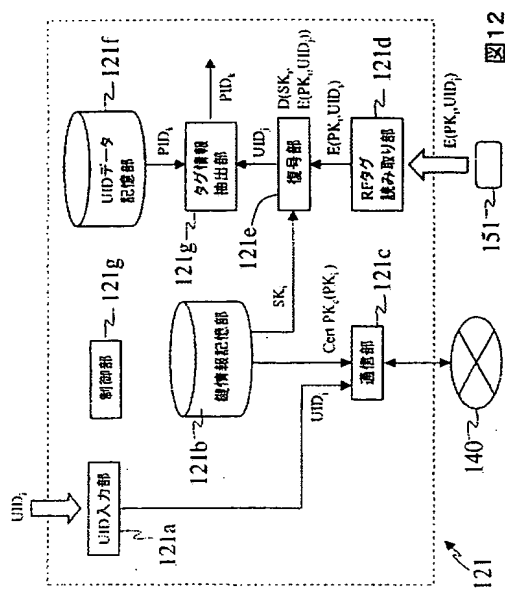


図12

【 図 1 3 】

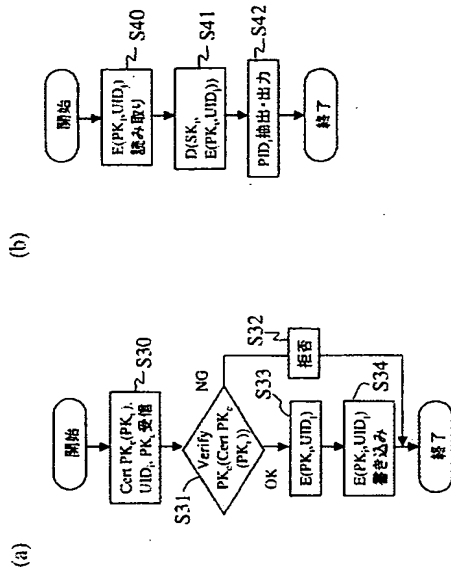


図 13

【 図 1 5 】

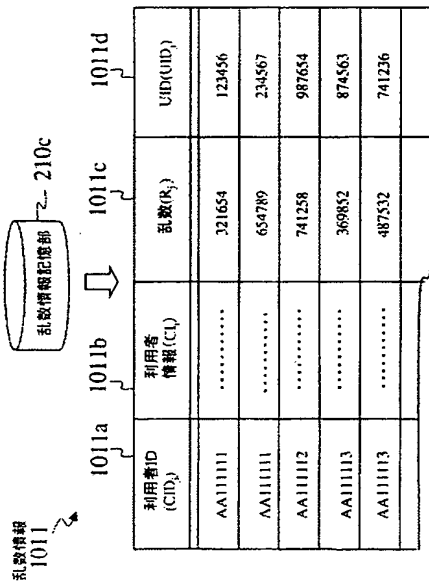


図 15

【 図 1 4 】

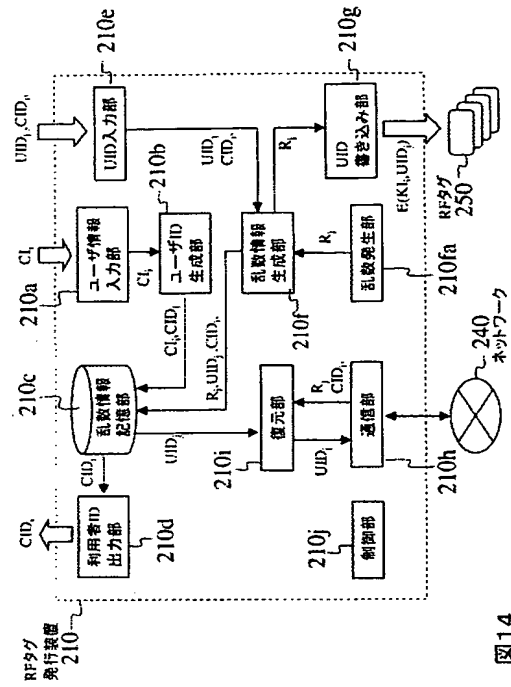


図 14

【 図 1 6 】

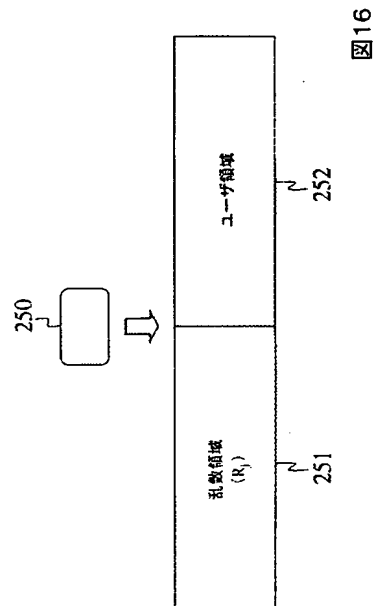
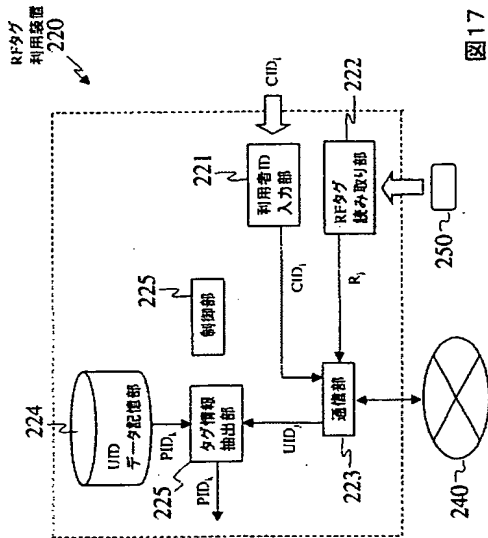
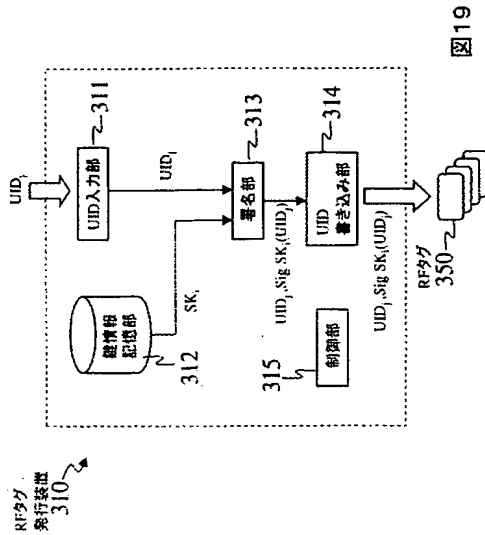


図 16

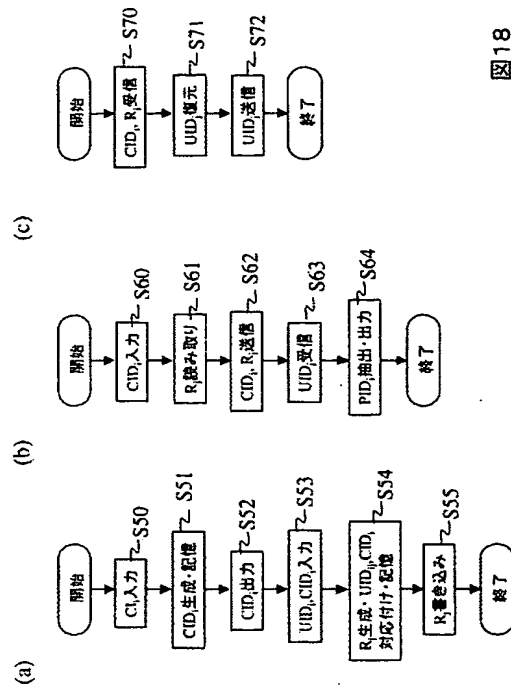
【 ㊦ 1 7 】



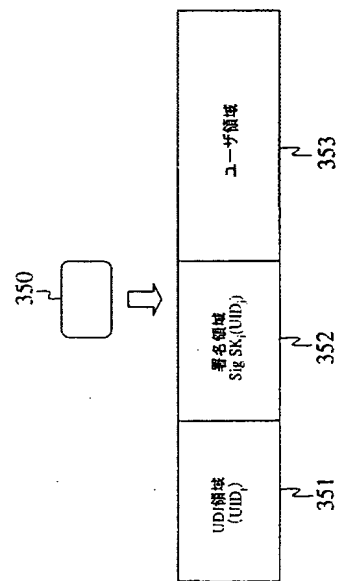
【 図 1 9 】



【 18 】

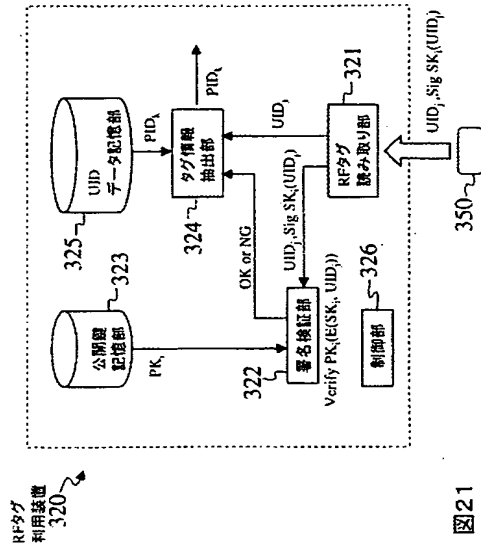


【 ㊦ 2 0 】

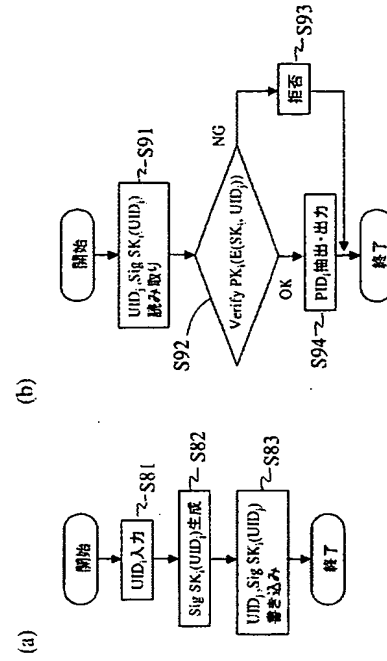


20

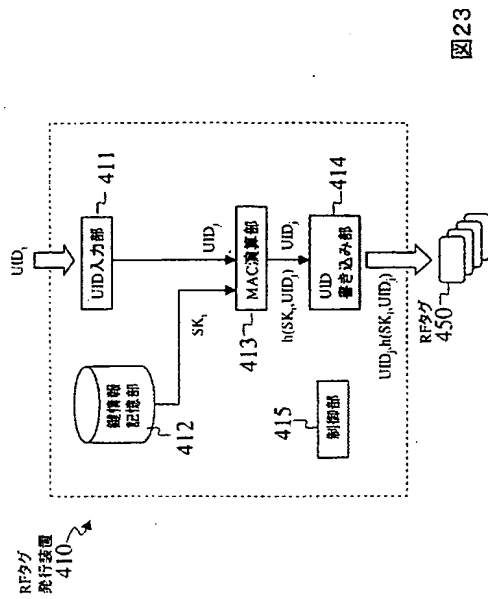
【 図 2 1 】



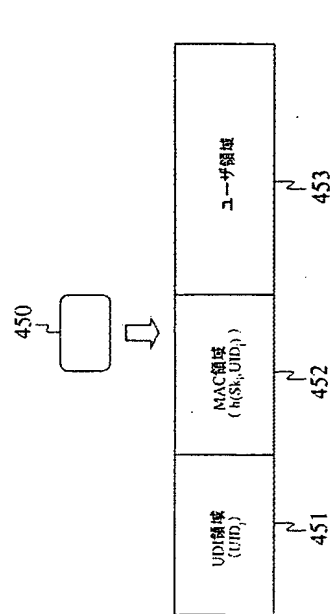
【 図 2 2 】



【 図 2 3 】



【 図 2 4 】



【 図 2 5 】

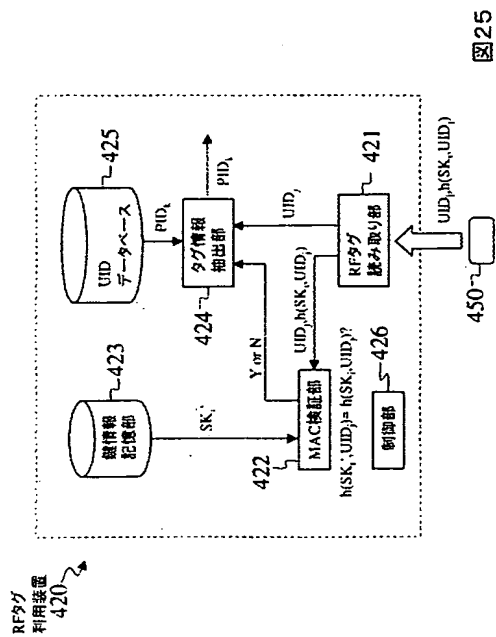


図25

【 図 2 6 】

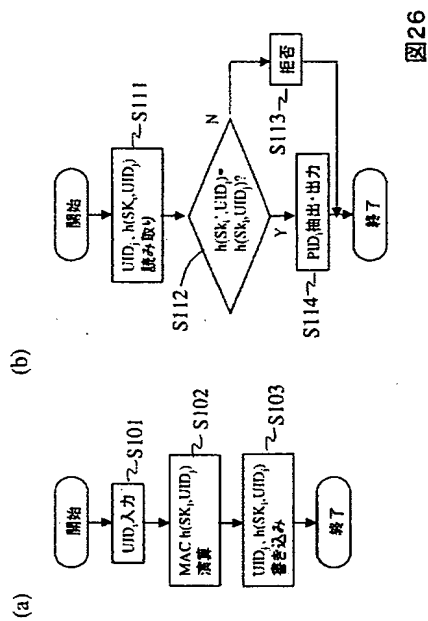


図26

【 図 2 7 】

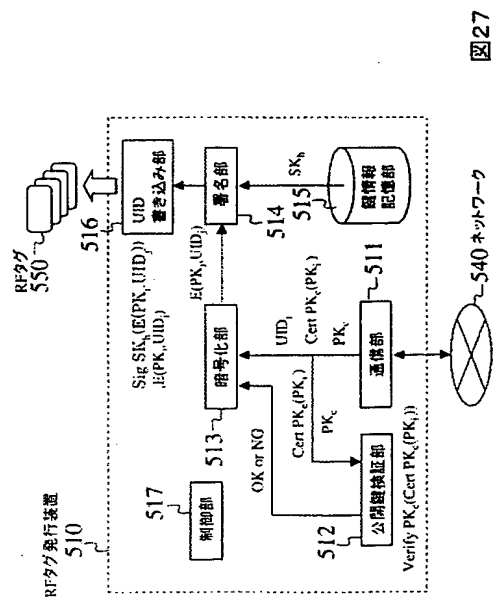


図27

【 図 2 8 】

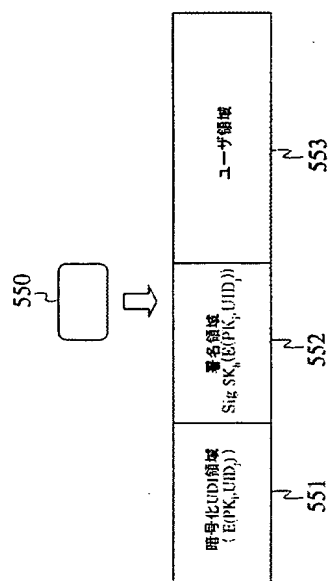
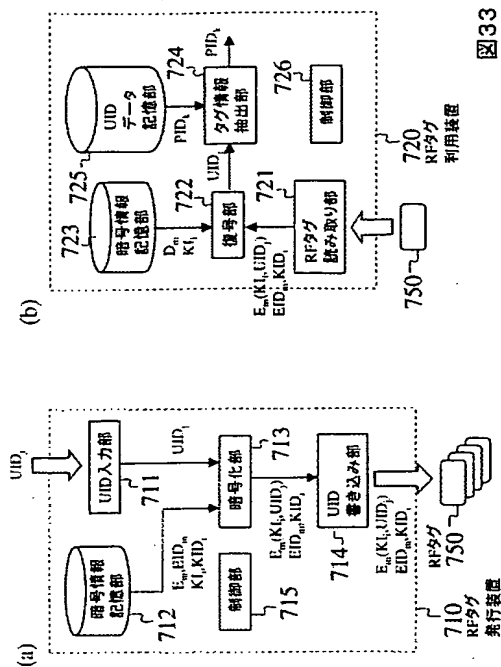


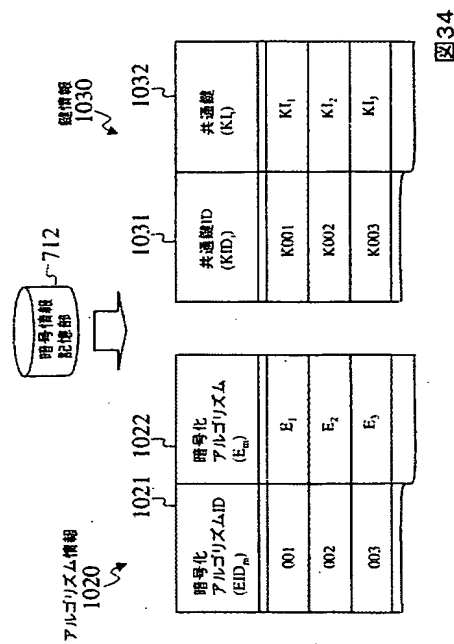
図28

【 ㊦ 3 3 】



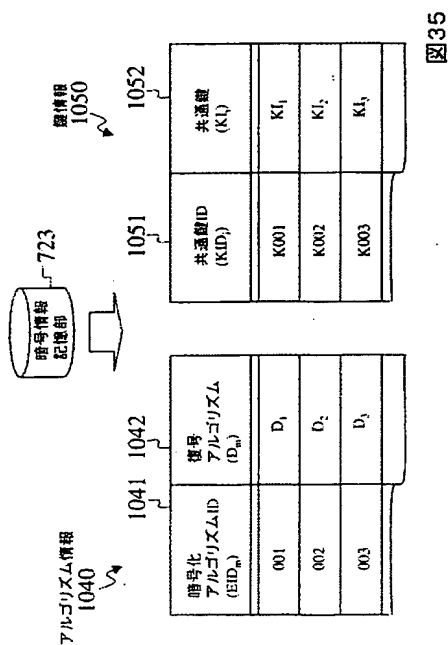
33

【 図 3 4 】



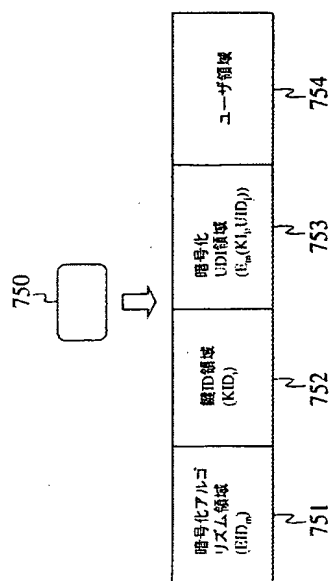
34

【 図 3 5 】



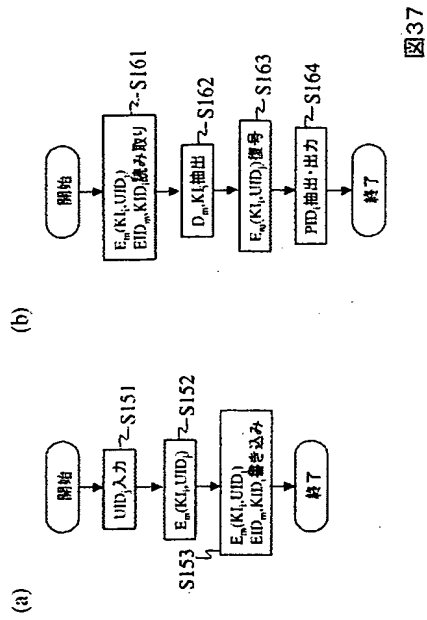
35

【 図 3 6 】

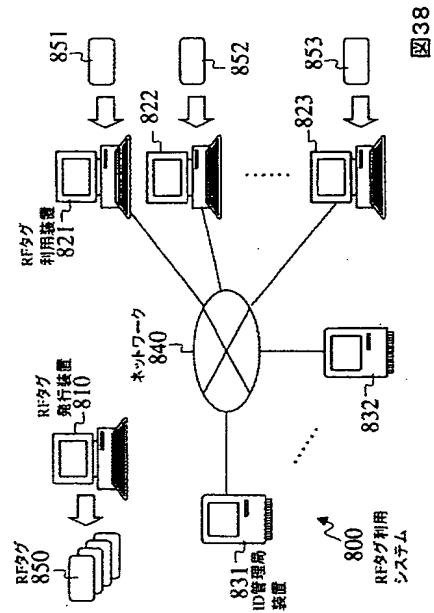


36

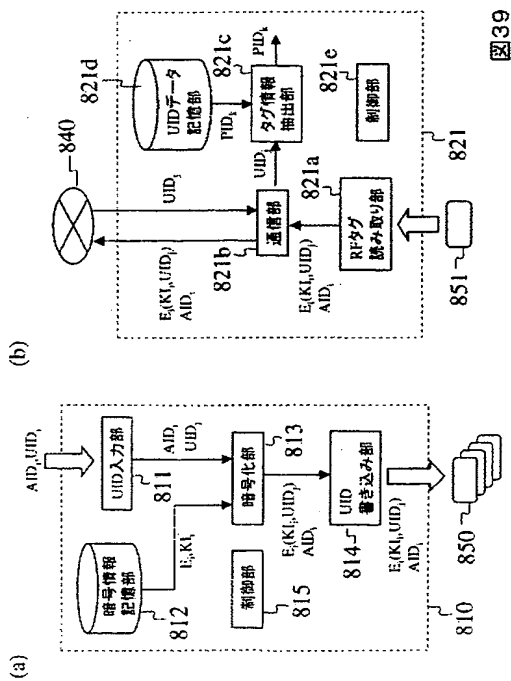
【 ㊦ 3 7 】



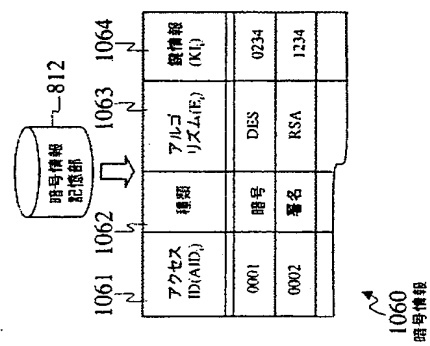
【 例 3 8 】



【 ㊦ 3 9 】



【圖 40】



40

【 図 4 1 】

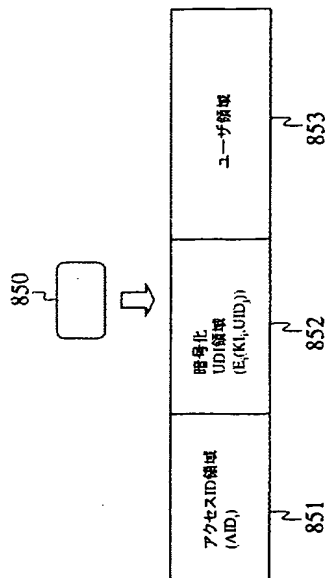


図 41

【 図 4 2 】

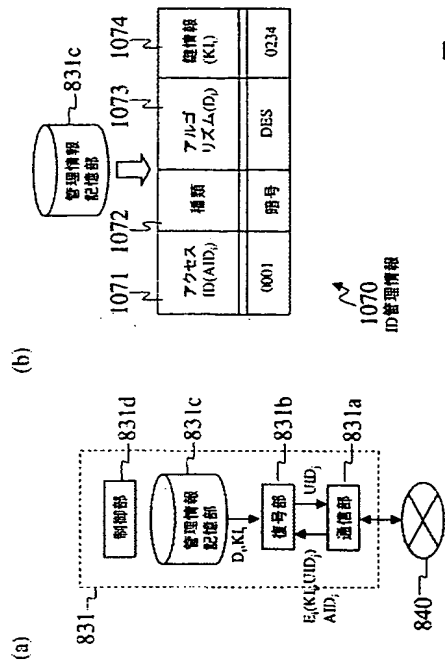


図 42

【 図 4 3 】

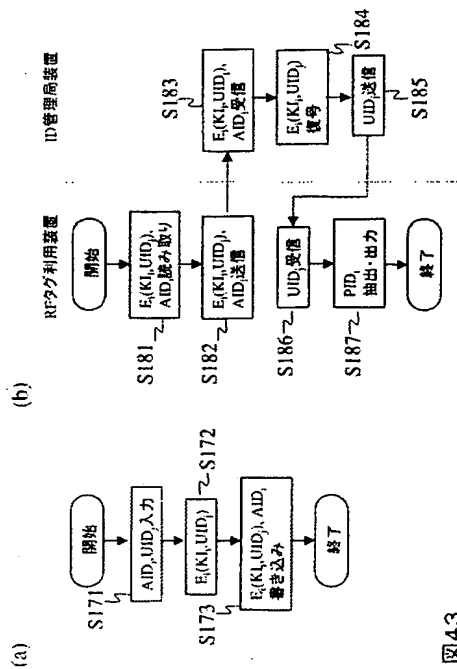


図 43

フロントページの続き

(72)発明者 星野 文学

東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

(72)発明者 藤村 明子

東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

Fターム(参考) 5B058 CA15 CA25 KA01 KA04 KA11 KA31 KA32 KA35

5J104 AA07 NA36 PA10

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.